THE LAW OF CYBER-SPACE

AN INVITATION TO THE TABLE OF NEGOTIATIONS

AHMAD KAMAL

UNITAR

United Nations
Institute of Training and Research

Published by the
United Nations Institute for Training and Research
Palais des Nations
CH 1211 Geneva 10
Switzerland

First Edition: October 2005
ISBN: 92-9182-038-8

PREFACE

This book is presented to the Member States of the United Nations by the United Nations Institute for Training and Research (UNITAR) as part of its programmes in the field of Information Technology.

It is, as the title indicates, an invitation to consider the importance of starting negotiations in a sector which has been much ignored over the past few years.

Hopefully, its importance and depth will be duly appreciated, and the material in it actually used for negotiations on a Law of Cyber-Space.

Marcel Boisard
United Nations Assistant Secretary-General
Executive Director, UNITAR

TABLE OF CONTENTS

FOREWORD

This book is a sequel to the earlier work on Information Insecurity, in which it had been argued that the absence of globally harmonized legislation was turning cyber-space into an area of ever increasing dangers and worries. In many ways, this situation is similar to the problems faced in dealing with the high seas, where the absence of consensus legislation was also creating an avoidable and acute vacuum. The international community finally woke up to the challenge, and started negotiations on the Law of the Sea. Those negotiations went on for almost a decade, but did finally succeed. The world is much better off as a result.

In the case of cyber-space, the challenge is far greater. The speed of change is phenomenal, the dangers affect all countries without exception, new shoals and icebergs appear every day, and global responses are sporadic or non-existent. There can be no doubt whatsoever that a globally negotiated and comprehensive Law of Cyber-Space is essential.

A complication arises from the fact that there are three distinct parties whose agreement would be necessary in any negotiations, namely, the governments, the private sector, and civil society. Each has an interest in the outcome, and each is a legitimate and absolutely essential stake-holder. Governments have the obvious power to legislate and to enforce laws. The private sector is the engine of all research and development in the sector of information technology, and knows the intimate details of the hardware and software on which its architecture is based. Civil society is the ultimate end-user, and benefits or suffers from its use and misuse. All three have somehow to be fully involved in the negotiations, in an atmosphere of mutual trust and respect, in which no one of the three tries to impose its weight on the other two.

The question is where these essential negotiations can be conducted. It would appesar that only the United Nations can provide the neutral and legitimate forum for this task. It is the only truly universal multi-lateral organization that we have, and its stamp of legitimacy is unequalled. Care would have to be taken, however, to ensure that the location of the negotiation in the United Nations is not interpreted as turning it into a purely inter-government negotiation. That will just not work. All three stakeholders must be full participants in the exercise.

This book is thus presented as a working manual for a tri-partite negotiation. It attempts to list the known aspects of the problem, to analyze the piece-meal manner in which different countries have addressed some of its component parts so far, and to offer some solutions for further work.

An effort has been made to identify the different known legal problems and to classify them under twenty-eight specific chapters. Chapters 01 to 16 form one part which describes *what* are the subjects of the criminal conduit

in cyber-space, while chapters 17 to 28 explain *where*, *why* and *how* these misconducts can fit into the present legal framework. The classification is rather arbitrary, and is only meant to help in slicing the overall problem into some component elements. Thre are overlaps and inter-linkages, which future negotiators would have to unravel.

The pattern followed for each of these chapters is identical. A first part attempts to identify the parameters of the problem, a second part brings together most of the existing texts on the subject, a third part tries to spot the loopholes that still remain to be plugged, and a final and fourth part suggests some possible solutions. The latter are merely suggestions, as it will be for the negotiators to agree on and determine the actual content of a comprehensive Law of Cyber-Space.

This analysis is, unfortunately, seriously constrained by the fact that technological advances in cyber-space are hurtling forward at break-neck speed. In fact not a day passes without the discovery of new facts, new dangers, new insecurities. That makes for a highly dynamic situation. As opposed to that, the book being presented is static, because it is being written and published at a specific point of time. Due note has thus to be taken of the need to compensate for the gap that will inevitably exist between this publication and all new developments.

A number of individuals have to be thanked for the enormous effort that has been expended in preparing this book. In the first place stand Professor Ehab Al-Shaer of the School of Computer Science, Telecommunications and Information Systems, Professor Katherine Strandberg of the College of Law, and Professor Patricia Szczerba of the School for New Learning, all from DePaul University in Chicago, and a large group of their students, who first researched the laws and regulations adopted by different countries. Then come two young students from Fairleigh Dickinson University in New Jersey, Kate Dumont and Max Burkey, who helped sift and classify the vast amount of material that had been gathered. Finally, my deepest and most grateful acknowledgement of the assistance received from Mr. Florin Butunoi, a young lawyer from Romania, currently, undergoing advanced studies at Seton Hall University in New Jersey, whose inputs have been invaluable.

The manuscript was reviewed by Professor Ehab Al-Shaer, Professor Katherine Strandberg, and Professor Barry Kellman, as also by Ambassador Henning Wegener, the Chairman of the Permanent Monitoring Panel on Information Security of the World Federation of Scientists. All gave valuable suggestions for improvement and I am most grateful to them for their time and effort.

INTRODUCTION

By any reckoning, the phenomenal growth of the global information technology infra-structure has been one of the most decisive events which distinguishes our contemporary times. In just over the past five years, the number of Internet users has sky-rocketed from 0.5 million to 6.5 million – a thirteen fold increase[1].

In the process, an entirely new universe has been created – the World of Cyber-Space. In many ways, this new frontier parallels the Wild West, with very few laws or norms to regulate human behavior, and innumerable outlaws only too willing to exploit the virgin territory of this vacuum.

It is increasingly clear that the benefits of this World of Cyber-Space cannot be enjoyed without drafting a comprehensive legislation, or without harmonizing the isolated laws which exist here and there.

Here are some reasons why it is necessary more than ever before to start work on this Law of Cyber-Space:

- Every day, more than 30,000 personal computers are being recruited into secret networks that spread spam and viruses[2].
- With the help of computers and access to the Internet, intellectual property continues to face high levels of piracy in key markets throughout the world. Economic damage is estimated at $25-$30 billion globally[3].
- Data on 50 million credit cards and personal information has been stolen in just the first half of 2005 in the USA alone.
- Twenty percent of people responding to a 2004 survey in the USA reported that they have personally been victims of identity fraud or theft. If this data is projected, the results suggest that close to 50 million individuals have already been victims of identity fraud or theft in this one country alone.
- An innovative and burgeoning sector of the economy – eCommerce – is now endangered. According to a recent survey, 64 percent of the people surveyed have decided against purchasing something on-line because of fears about the leakage and misuse of personal information.
- In other recent surveys[4], it has been shown that Internet attacks continue to be the most prominent threat to service providers and enterprise networks, causing the most devastating damage for current businesses. The average losses reported by the firms as a

1 http://www.internetworldstats.com/stats.htm

2 http://news.scotsman.com/topics.

3 www.iipa.com/pressreleases/2005_ Apr29_Press_Release_USTR_301_Decisions.pdf

4 CSI/FBI Computer Crime & Security Survey of 2004 and Arbor Networks Survey of Internet Infrastructure of 2005

result of Internet attacks represent about 60% of all other losses. Internet attacks now outpace what used to be the most costly threats formerly, such as theft of proprietary information. About 40% of firms receive as many as 100 attacks a month, and 80% of these are high magnitude virus and denial of service attacks.

- Spam now accounts for 45% of all e-mails, or 15 billion messages every day. The world wide cost to business stands at a staggering total of $20 billion a year in lost productivity and technology expenses. At the projected rate of growth, the number of daily spam messages will rise to more than 50 billion by 2007, with costs touching almost $200 billion per year.
- A new technological threat now exists in the domain of terrorism. Although terrorists have typically used traditional methods of physical attack (explosives, kidnappings, and hijackings), their attention will inevitably move with increasing frequency toward cyber-terrorism. A large part of the global infrastructure will be vulnerable to such attacks (pipelines, power plants, transportation, communications systems, and other hard assets) because of their high reliance on cyber-technology.
- Cyber-war is now a real danger. If ordinary individuals have understood the opportunities inherent in the damage potential of information technology, states will obviously plan even more devastating uses for this weapon.

It is therefore essential to agree on a Law of Cyber-Space[5]. In negotiating and adopting such legislation due account has to be taken of the following essential aspects:

- Cyber-space is part of the common heritage of mankind. Access to its benefits is a legitimate right for all peoples. The object of legislation is not to limit that right, but only to limit or eliminate all abuses of that right.
- No negotiation would be possible or durable without the full participation of all three stake-holders, namely, governments, the business sector, and civil society. It would be a serious error to believe that governments alone can negotiate the elements of a comprehensive legislation.
- Once all three stake-holders are brought together, the overall endeavor must be to identify each and every one of the dangers that exist, and then to agree on legislation which addresses each of these dangers.

5 Toward a Universal Order of Cyber-Space: Managing Threats from Cyber-crime to Cyber-war- Report and Recommendations, World Federation of Scientists, Permanent Monitoring Panel on Information Security. August 2003.http:www.//it is-ev.de/infosecur.

- Given the completely porous nature of boundaries and frontiers in the face of advances in information technology, it would be essential to harmonize laws globally so that, to the maximum extent possible, all loopholes are plugged. The current divergences in cyber-legislation in different states need to be noted.
- The power of information technology as a tool for economic and social progress must not be sacrificed at the altar of unnecessary controls and censorship. Access to knowledge is by far the greatest benefit of this technology, and no efforts must ever be made to limit that access.
- The agreed objective of global legislation must nevertheless ensure a proper balance between freedom of expression and an effective fight against the dissemination of all views of a racist or humanly demeaning nature. While the legislation must respect privacy and anonymity as important values, any abuse of these values must be dealt with unequivocally.

CHAPTER 01. DEFINITIONS

Definitions are essential in any law or treaty. A problem that is specific to definitions in the field of information technology arises from the rapid evolution which has characterized it over the past few decades, with new words and new concepts emerging every year, and even every day. Definitions thus suffer from their static nature in a highly dynamic environment. So, Time is a problem.

A further complication arises from the disparities in technology and in linguistic norms that distinguish different countries and regions in our geographical globe. So, Space is also a problem.

The following definitions, which are neither complete nor exhaustive, are nevertheless proposed to help in a better understanding of the parameters of the problem and for possible use in any future negotiations:

Access control

Actions taken to permit the ordinary use of the components of a communications system. The tasks performed by hardware, software and administrative controls to monitor system operation, ensure data integrity, perform user identification, record system access and changes and grant users access.

ACH

Automated Clearing House-a funds transfer system that was developed as an electronic payment alternative to checks.

Address

A location that can be specifically referred to in a program. It can refer to a storage location, a terminal, a peripheral device, a cursor location or any other unit or component in a computer network.

Addressee of a data message

A person who is intended by the originator to be the ultimate recipient of a data message, but does not include any person acting as an intermediary with respect to that data message.

ADR-Alternative Dispute Resolution

The generic name given to several dispute resolution processes and techniques which stand outside the traditional mainstream of formal state jurisprudence.

Advanced electronic signature

An electronic signature which meets the following requirements: (a) it is uniquely linked to the signatory; (b) it is capable of identifying the signatory; (c) it is created using means that the signatory can maintain under his sole control; and (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Anonymity

Lacking any distinguishing feature which can enable the identification of its originator.

Archive

A procedure for transferring information from an on-line storage diskette or memory area to an off-line storage medium.

ATM Cards

A type of Payment Card used in an Automatic Teller Machine, that deducts expenditures directly from an individual's bank or credit card account account.

Automated computer system

Means a computer program or an electronic or other automated means used to initiate an action or respond to data messages or performances in whole or in part, without review or intervention by a natural person, each time an action is initiated or a response is generated by the system.

Automated data file

Any set of data undergoing automatic processing.

Automatic processing

Operations carried out in whole or in part by automated means for the following: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination.

Backup

The provision, logical or physical, of facilities which can speed up the process of restart and recovery following failure. Facilities may include duplicated files of past transactions, duplicated processors, storage devices, terminals, telecommunications hardware switches to facilitate the recovery of data which may have been inadvertently lost or erased.

Bit

The smallest unit of coded information, normally stored and transmitted in binary format by computer systems.

Bit map

A matrix of dots, all of the same density, that form an image.

Bot

A software agent which is part of an infiltrated software program, which actis as a real person performing tasks such as retrieving and delivering information, and automating repetitive tasks.

Broadcast

The simultaneous transmission of an electronic message to a number of receiving locations.

Byte

A contiguous sequence of a fixed number of bits used as a unit of storage measurement in computers, regardless of the type of data being stored.

Cache memory

A very fast memory which can be accessed more quickly than regular RAM (random access memory). As a microprocessor processes data, it looks first in the cache memory, and if it finds the data there from a previous reading, it does not have to retrieve it from the RAM in a more time-consuming manner.

Certificate

An electronic attestation which links signature-verification data to a person and thus confirms the identity of that person.

Certification-service-provider

An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.

Civil Liberties

Personal rights which are protected from the arbitrary power of governments, such as, the right to life, the right to privacy, the right to a fair trial, freedom of speech and freedom of assembly. These are usually guaranteed and protected by a constitution or by adherence to an international treaty.

Civil Remedies

The means by which a right is enforced or by which the violation of a right is prevented or compensated. Also, the means employed to enforce a right or to redress an injury.

Communication

Any information exchanged or conveyed between a finite number of parties by means of a publicly available electronic communications service.

Competition authority

A regulatory body that is responsible for the supervision of general competition rules.

Compression

Techniques to reduce the number of bits required to represent information in data transmission or storage, thereby conserving bandwidth and/or memory.

Computer data

Any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program which can enable a computer system to perform a particular function.

Computer system

Any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.

Controller of the file

The natural or legal person, public authority, agency or any other body, competent under national law to decide what should be the purpose of the

automated data file, or which categories of personal data should be stored, or which operations should be applied to them.

Copyright

A form of state-sponsored protection provided to the authors of original works. Works can include literary, dramatic, musical, artistic, or other intellectual works, both published and unpublished.

Copyright owner

The owner of the particular rights and protections with respect to a copyright.

Cyber-hooliganism

Computer network related mischief, such as defacing websites or releasing a virus or a worm, without necessarily causing any serious disruption or widespread panic or terror for the general population.

Cyber-stalking

The use of images, signs, language, or other similar means for the willful purpose of systematically threatening, harassing, intimidating, tormenting or embarrassing directly or indirectly another person, either through electronic devices or by e-mail or over the Internet.

Cyber-terrorism

Attacks and threats of attack against computers, networks, and the information stored therein, with the objective of intimidating or coercing a government or its people in furtherance of political or social objectives.

Cyber-war

The deliberate use of information warfare by a state, using weapons such as electro-magnetic pulse waves, viruses, worms, Trojan horses, etc., which target the electronic devices and networks of an enemy state.

Data communications

The transfer of information between a source and a destination via one or more data links, using appropriate protocols. Transmission and reception of such data often includes operations such as coding, decoding and validation.

Defamation

The delict of making a false statement of fact that injures someone's reputation.

Denial of service attacks

Distributed Denial of Service (DDoS) attacks are aimed at denying authorized persons normal and legitimate access to a computer or computer network by overwhelming the latter with non-relevant messages. These attacks may be launched from a single computer or from millions of computers around the world.

Distance contract

Any contract concerning goods or services concluded between a supplier and a consumer under an organized distance sales or service-provision scheme run by the supplier.

Domain name

Any designation in letters and/or numbers which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority, as part of an electronic address on the Internet.

Electronic Data Interchange (EDI)

The computer-to-computer exchange of business data in a standard format.

Electronic device

A device that accomplishes its purpose electronically by transferring signs, signals, writings, images, sounds, data, or intelligence of any nature, using wire, radio, or computer, and thorugh a system which can be electro-magnetic, photo-electric, or photo-optical.

Electronic evidence

Documents originating in a native, or computer-generated, format and containing metadata.

Electronic mail

Any text, voice, and sound or image message sent over a public communications network which can be stored in the network or in the recipient's terminal equipment until it is collected by the recipient.

Electronic mail address

A destination, consisting of a unique user name or mailbox and a reference to an Internet domain, whether or not displayed, to which an electronic mail message can be sent or delivered.

Electronic signature

Identification data in electronic form which is attached to or logically associated with other electronic data to serve as a method of authentication.

Electronic-signature product

Hardware or software, or the relevant components thereof, which are intended to be used by a certification-service-provider for the provision of electronic-signature services, or are intended to be used for the creation or verification of electronic signatures.

Encryption

The translation of data into a secret code which subsequently requires a secret key or password that enables its decryption. Unencrypted data is called plain text while encrypted data is referred to as cipher text.

Extension

A suffix, typically three characters long, following a "dot" in a filename, which allows computer users and programs to recognize a file's format; for example, resume.doc.

Extradition

A formal process by which a criminal suspect held by one government is handed over to another government for trial or, to serve a sentence.

Freedom of speech

The liberty to freely say what one pleases, as well as the related liberty to hear what others have stated. Also the freedom to create and distribute movies, pictures, songs, dances, and all other forms of expressive communication.

Forging data process

Any operation upon personal data for the purpose of making a false personal identification document.

Hacking

A generic term for all forms of unauthorized access to a computer or a computer network.

Harassment

Any intentional, substantial and unreasonable intrusion into the private life of a person that causes the person to suffer mental distress.

Hidden text

Editorial comments or text editing changes which are electronically concealed until the reader operates a separate process to reveal them.

Identification means

Any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any name, social security number, date of birth, driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; unique electronic identification number, address, or routing code; telecommunication identifying information or access device.

Image File Format

A representation (usually binary) used by a computer system as an agreed format to store an image or for displaying graphics.

Independent regulator

A sector specific independent regulator that is distinct from the Ministry as well as other telecommunications operators.

Information system

A system for generating, sending, receiving, storing or otherwise processing data messages.

Infringement

Illegally entering or trespassing. In intellectual property matters, the incorrect usage of a patent, writing, graphic, or trademark without permission or notice.

Intellectual property

New ideas, original expressions, distinctive names, and appearance that make products unique and associated with the inventor.

Internet Protocol (IP)

The protocol used to route a data packet from its source to its destination over the Internet.

Internet Service Provider (ISP)

An organization that provides Internet access and related services to users.

Jurisdiction

The ability to subject an individual to adjudication in a forum.

Liability

The legal responsibility that one has over acts or omissions. If a person or entity fails to meet such responsibilities becomes open to a lawsuit for damages that may result.

Location data

Any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.

Looping

The act of repeating an instruction set until a specific condition is met. An infinite loop occurs when the condition will never be met, due to some inherent characteristic of the loop. Many programs loop forever waiting for servicing requests.

Malicious code

A software or a code which modifies or destroys data, steals data or allows unauthorized access, or exploits or damages a system in a manner not intended by the user.

Means of distance communication

Any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the conclusion of a contract between those parties.

Mediation and Arbitration

Traditional methods of dispute resolution for deciding controversies between individuals, businesses and countries.

Metadata

Data about data; descriptive information and statistics embedded in a given computer file.

Ministry of Telecommunications

A government agency that is responsible for policy making in the telecommunications sector.

Native File Format

The file format in which a computer file was originally created.

Obscene

Such indecency as is calculated to promote the violation of the law and the general corruption of morals, and which is perceived as such.

Online Dispute Resolution

A type of dispute resolution in which technology is used to facilitate the resolution of disputes between parties outside traditional jurisdiction.

Operator of a means of communication

Any public or private natural or legal person whose trade, business or profession makes distance communications available to suppliers.

Originator of a data message

A person by whom, or on whose behalf, a data message is sent or generated prior to storage, but not including a person acting as an intermediary with respect to that data message.

Ownership of a copyright

An assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time or place of effect, but not including a non-exclusive license.

Patent

The grant of a property right to the inventor, issued by the authorities.

Personal data

Any information relating to an identified or identifiable individual.

Personal identification

Any information related to an identified or identifiable natural person.

Personal Identification Number (PIN)

A personal identification number created for the exclusive use and identification of an individual.

Portable Document File (PDF)

An image format created by Adobe Systems that allows users to view a file with its intended formatting without any need for any further action by the program in which the original file was created.

Privacy

The ability of an individual or group to stop personal information from becoming known to people other than those whom they choose to give the information to.

Recipient

An authorized user of the electronic mail address to which the message was sent or delivered.

Record

Information that is inscribed on a tangible medium, or that is stored in an electronic or other medium, and is retrievable in perceivable form.

Service provider

Any public or private entity that provides to users of its service the ability to communicate by means of a computer system, or any other entity that processes or stores computer data on behalf of such a communication service or users of such a service.

Signatory

A person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity whom he represents.

Signature-creation data

Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;

Signature-creation device

Configured software or hardware used to implement the signature-creation data.

Signature-verification-data

Data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.

Signature-verification device

Configured software or hardware used to implement the signature-verification data.

Software

A set of statements or instructions used by computers in order to bring about desired results.

Sovereignty

The right to exercise supreme authority over a geographic region or a group of people.

Secure Socket Layer (SSL) protocol

A protocol which anables authentication and communications privacy over the Internet by using cryptography.

Tax

Any charge imposed by any governmental entity for the purpose of generating revenues for governmental purposes, and which is not a fee imposed for a specific privilege, service, or benefit conferred.

Telecommunications regulator

A regulatory body or a ministry that is responsible for the supervision of telecommunication regulations.

Terrorism

The use of violence for political objectives and for the purpose of sowing fear within a target population.

Threaten

A statement of intent or an action intended to place a person in reasonable fear of physical or psychological safety.

Trademark

A word, name, symbol or device which is used in trade to indicate the source of goods to distinguish them from the goods of others.

Traffic data

Any computer data relating to a communication by means of a computer system, indicating the origin, destination, route, time, date, size, duration, or type of a communication.

Transactional mail message

Any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service.

Trojans

A program which pretends to do one thing while actually doing something completely different.

Unauthorized access

Intrusion into a protected computer without due authorization.

User

Any natural person using a publicly available electronic communications service, for private or business purposes.

Uniform Resource Locator (URL)

The specific global address of documents and other resources on the World Wide Web.

Value added service

Any service which requires the processing of traffic data or location data other than traffic data beyond what is necessary for the transmission of a communication or the billing thereof.

Value added tax (VAT)

A tax which corresponds only to the "added" value of goods or services, and not to the whole value of such goods and services.

Virus

Code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program, and may damage hardware, software, or data.

Voluntary accreditation

Any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification-service-provider concerned, or by the public or private body charged with the elaboration of and supervision of compliance with such rights and obligations;

Web Pages

Pages on the World Wide Web with links which enable navigation from one page or section to another.

Website

A collection of web pages accessible on the Internet.

Worm

A self-contained program that is able to spread functional copies of itself or its segments to other computer systems.

CHAPTER 02. THE RIGHT TO ACCESS

The Problem

The exploding use of information systems and networks has led to an increasingly interconnected world. Computer networks now support critical infrastructures such as energy, transportation, and banking and finance, and play a major part in how companies do business, how governments provide services to citizens and enterprises, and how people communicate and exchange information. The number and nature of technologies has multiplied and will continue to grow, as has the nature, volume, and sensitivity of information that is moving from place to place. At the same time, these information systems and networks are being exposed to a growing variety of new threats. Electronic commerce and the marketplace cannot thrive without strong and safe information networks which the public can trust. One element of assuring such secure networks is a comprehensive legal framework to deter, identify, and prosecute attacks on them.

Criminals, like businesses, governments, and individuals, take advantage of the ability of computers to store large amounts of information. The use of computers as storage devices generally does not require the creation of new substantive laws, but the growth of electronic evidence may require a country to consider amendments to laws regulating the access to such evidence by enforcement agencies.

A computer can also be the target of criminal activity. Commonly called network crimes, this activity involves attacks on the confidentiality, integrity, or availability of computer systems or information. Criminals undertake these attacks to acquire information stored on the target system, to control the target system without authorization or payment, to delete or modify data, or to interfere with the availability of a computer or information on it. Often these attacks result in the theft of information or monetary loss to the owner of the victim computer. Criminal activities included in this category are computer intrusions, the release of viruses and other malicious code, website defacements, and denial-of-service attacks that impair the availability of computer systems or data.

A computer intrusion, or access without right (also called *a hack)*, occurs when an individual trespasses into a computer or part of a computer system to which that person is not entitled to have access. Such intruders may be divided into two categories: persons who attack from outside the network and wrongfully access a computer without authorization, and persons who are insiders and thus have authorization to access specific portions of the network but intrude into other parts of it by exceeding authorized access. Prohibiting computer intrusions is the heart of any network crimes law[6].

6 Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo, National Defense University Press 1998

Since most Internet users do not have enough of a technical background to understand exactly how Internet tools work, privacy exploits have become entrenched in the online environment.

First among the privacy-intrusive practices is the use of *cookies* - a small file downloaded from a web site onto the visitor's home computer. The cookie then remains on the visitor's hard drive for whatever purpose the designer requires, either to confirm a session visit (for audit purposes), to verify the identity of the visitor or, in some cases, to execute a program without the permission of the owner. While unauthorized access to a computer is a crime, the cookie technology bypasses the criminal law by being voluntary. If one sets up the web browser program to refuse cookies then no intrusion occurs. It is therefore arguable by the designers of cookie-ridden sites that if individuals choose not to refuse cookies then they are volunteers for whatever consequences follow.

Web-bugs are another secret technology, usually existing as a one pixel picture file on a web page, too small to be seen with the naked eye. The web bug is therefore loaded by the visitor's web browser unintentionally, giving the web site a separate log file of the Internet addresses of visitors to the page in question. A web site can therefore use web-bugs to spy on the personal details of visitors to the web site without the visitor even being aware that this has happened.

The web is also mined for e-mail addresses and other personal details by *web-spiders*, programs which search the Internet for web pages which may or may not be linked to search engines. Any page in a web directory can be reviewed by these programs, whether or not they are linked to search engines and indices. These programs, used by search engines to retrieve links, also provide a rich vein of personal data, suitable for profiling or sale to commercial and security interests.

More and more web-sites now demand registration, or proof of identity. These demands have no function for the use of a web site, but are instead motivated by a new revenue stream based on the aggregation and sale of personal information by web sites. In the absence of privacy legislation outlawing such secret data mining, even reputable companies find the lure of the trade in private information irresistible, and seek to incorporate the sale of personal details in the business model. These privacy abuses are often concealed by self-serving privacy policies which, deep in the fine print, permit the site owner to collate and sell personal information to others.

The online environment needs a higher degree of privacy than the offline world because only an electronic means of verification of identity is possible in cyber-space. The leakage of personal information can thus lead to effective impersonation, fraud, cyber-stalking and theft of confidential information[7].

7 www.nswscl.org.au/journal/43/Heitman.html

Obtaining access to a computer by exceeding authorized access, on the other hand, refers to the activities of insiders who, by employment or some other relationship, have authority to access certain areas of a network, but who then use that authorized access to obtain privileges beyond those to which they are entitled. Like outsiders, such users then access stored files that they would not normally be able to access, intercept communications of other users, delete or modify files, or cause the system to crash. Such intrusions are carried out most frequently by disgruntled employees.

The Existing Texts

Many countries criminalize the act of gaining unauthorized access or exceeding authorized access to a computer, even if the individual does nothing more. Other countries, however, require proof that the hacker took some additional action.

FRANCE[8]

Article 323-1 of the French penal code (1994) contains the following provision:

Fraudulently obtaining or maintaining access to the whole or part of a system for automated data processing is punishable by [imprisonment and a fine].

JAPAN

Japan passed a computer crime statute in 1999 with the following provision:

Article 3. No person shall conduct an act of unauthorized computer access.

The act of unauthorized computer access mentioned in the preceding paragraph means an act that falls under one of the following items:

1. An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person's identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code);

2. An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item);

3. An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another

8 www.legifrance.gouv.fr

specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication line, any information or command that can evade the restrictions concerned.

Japanese law does not criminalize unauthorized access to a computer unless the intruder has circumvented some security measure. By limiting the scope of the statute in this way, however the law may allow a hacker who causes severe damage to a computer system to escape punishment where the owner of the system – perhaps through inexperience or ignorance, failed to secure it.

EUROPE

Article 2 of the Council of Europe Convention on Cyber-crime addresses this criminal activity as follows:

Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Many countries have used varying language to criminalize obtaining data during the unauthorized access of a computer or the exceeding of authorized access. In many situations, intrusions occur not as an end in themselves but as part of a larger criminal scheme. Such schemes can include any number of other crimes. Criminals may hack into a computer in order to obtain information that they can use to commit some other crime, such as obtaining credit card or bank account numbers in order to make fraudulent purchases or to transfer funds fraudulently.

USA

The United States has a similar provision that makes it an offense to intentionally access a computer without authorization, or exceed authorized access, and thereby obtain information. This statute does not require that the hacker download a complete file to some permanent medium; obtaining information includes merely viewing it on the screen of a remote computer.

The United States[9] has created special statutes to criminalize computer intrusions where the hacker breaks into the computer to further a particular crime.

Section 1030(a) (4) of title 18 of the United States Code states in full:

Whoever ... knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing

9 18 USC. § 1030(a)(4) (US), available at http://www.cyber-crime.gov/1030_new.html.

obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period....

UK

Computer Misuse Act 1990 regulates the Computer misuse offences.

Unauthorized access to computer material:

1. A person is guilty of an offence if:

a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer;

b) the access he intends to secure is unauthorized; and

c) he knows at the time when he causes the computer to perform the function that that is the case.

2. The intent a person has to have to commit an offence under this section need not be directed at

a) any particular program or data;

b) a program or data of any particular kind; or

c) a program or data held in any particular computer.

3. A person guilty of an offence under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

THE NETHERLANDS

The Netherlands has enacted a two-tier system, whereby accessing a computer without authority carries a maximum sentence of six months imprisonment, while accessing a computer and copying data carries a maximum sentence of four years imprisonment.

Article 138-a) of the penal code of the Netherlands has the following provisions:

A person who intentionally unlawfully intrudes into a computerized device or system for storing or processing data or a part of such a device or system is guilty of computer intrusion and liable to a term of imprisonment of not more than six months or a fine of the third category, where he: thereby breaches any security, or gains access by technological means, with the help of false signals or a false key, or by assuming a false capacity.

Computer intrusion is punishable by a term of imprisonment of not more than four years or a fine of the fourth category, where the offender subsequently copies the data stored in a computerized device or system, to which he has gained access unlawfully, and records such data for his own use or that of another.

The Loopholes

The increased incidence of trans-border hacking, as well as the use of looping[10] by hackers to hide their identities, must force legal systems to adapt in creative ways. For example, countries must reexamine polices and legal rules relating to extradition to assure that no country will provide a safe haven for

10 www.cybersecuritycooperation.org/moredocuments/ Drafting%20Cyber-crime%20Laws/SubstantiveLawsText.doc

hackers. In addition, if a hacker in one country breaks into bank computers in several other countries, it may make more sense for the hacker's home country to vindicate the rights of the victim's world wide by prosecuting the hacker for all of these crimes at one time, rather than have the hacker undergo a separate trial in each jurisdiction.

At a minimum, each country should have the maximum flexibility to prosecute hackers located both inside and outside of its borders. In particular, domestic laws should criminalize attacks on computers inside a country's borders regardless of whether the criminal is located inside or outside of the country. At the same time, each country's laws should allow for prosecution of domestic offenders who attack computers located in other countries. If such a domestic prosecution is unavailable, the law and treaties of that country must allow for extradition of such individuals to the country in which the victim is located. Moreover, each country's procedural laws must be capable of supporting the investigation and prosecution of individuals in foreign countries by collecting and sharing evidence of the crime with foreign law enforcement agencies and prosecutors.

There are as many different frameworks for punishment of network crime offenses as there are countries with such laws[11]. While there is no single correct answer to the question of how severe punishment should be for the various offenses, lawmakers should create punishments severe enough to deter and punish the invasions of privacy, thefts of information, and monetary and other harms that result from this misconduct. This deterrence and punishment usually includes fines, meaningful periods of incarceration, and restitution to victims.

Many national network crimes laws do not separate victims into categories; instead they simply equate all computers to define the specific offenses. Lawmakers may decide that certain computers are simply more sensitive, necessitating increased penalties for crimes involving them.

The Suggested Solution

In order to better protect computers and computer systems, and to improve the efficacy of the future law with regards to computer related crimes, any person who accesses a protected computer without authorization, or exceeds authorized access, knowingly and intentionally, should be punished. Even an attempt to access a computer or computer system without due right should be also incriminated. Depending on the losses and the social danger that is posed, the unauthorized access of a computer or computer system must be punished with proportionate fines and imprisonment. To be effective, the above recommendation must be implemented globally through the instrument of legal extradition.

11 http://www.nswscl.org.au/journal/43/ Heitman.html

CHAPTER 03. ANONYMITY

The Problem

Anonymity is the state of not being identifiable within a specific set. When referring to human beings, we say that a person is anonymous when the identity of that person is not known. Being anonymous is a result of not having one's identity, characteristics or significant features disclosed. This may be simply because the person was not asked, as in an occasional encounter between strangers, or because the person is unable or unwilling to tell. Often times the information is simply unavailable, and as a result, the correlation between the individual and the action is not possible.

As electronic communications technology becomes widespread among increasingly international populations of computer users, one of the most hotly-debated questions is how to maintain the benefits of free discourse while simultaneously restricting antisocial communications and behavior on the Internet. The debate is complicated by the international and intercultural dimensions of communications today[12]; what is viewed as freedom in some parts of the world is perceived as licencious in other communities. Conversely, what are seen by some as attempts to impose civility on international discourse are sometimes rejected as gross interference in freedom of speech by others. The challenge then for each society, and implicitly for global society, is to find out just how free we want ourselves and others to be.

At the heart of much of the debate over the advisability and possibility of imposing limits on behavior in cyber-space is the question of identity. Some of the most egregious abuse of cyber-space is attributable in part to the ease of concealing identity, using no names or false names. As a result, malefactors can often escape almost all of the consequences of their actions.

There are two different kinds of anonymity on the Internet: true anonymity and pseudo-anonymity[13]. Dialogue on the issues of anonymity legislation suffers on account of this lack of distinction between true anonymity and pseudo-anonymity.

True anonymity means that the identity of a person acting in a truly anonymous manner cannot be definitively discovered through any amount of diligence. Attempts can be made to discover the identity of the sender through inference, but any concrete trail of clues betraying the message sender has been erased by circumstance, the passage of time, or by the sender herself. Although some forms of truly anonymous communication, such as political speech, are considered valuable, this form of anonymity has exceptional potential for abuse because the senders of a message cannot be held accountable for their actions.

Pseudo-Anonymity in communication, on the other hand, is inherently traceable. Though the identity of the message sender may seem truly

12 http://faculty.ncwc.edu/toconnor/410/cyber-spacelaw.htm
13 http://www2.norwich.edu/mkabay/overviews/anonpseudo.htm

anonymous, because it is not easily uncovered or made readily available, it is possible to somehow discover the identity of a pseudo-anonymous message sender. Pseudo-anonymity has significant social benefits; it enables citizens of a democracy to voice their opinions without fear of retaliation against their personal reputations, but it forces them to take ultimate responsibility for their actions should the need somehow arise.

Anonymous [14] communication can be conducted through anonymous remailers. An anonymous remailer is a service that receives an email, strips it completely of the true sender's identifying information, and forwards the message to the email address specified by the sender. With some experience, a person can use anonymous remailers to send untraceable, truly anonymous messages.

The Existing Texts

Freedom has its consequences. Since attaining true anonymity in cyber-space is relatively easy, the medium is prone to abuse. Abuses of anonymity lead to increased costs for individuals, businesses, courts, and society. Not surprisingly, legislatures have begun to respond to this challenge.

Despite the fact that no one sovereign authority controls cyber-space, it is nevertheless not an ungoverned and lawless frontier; many actions in cyber-space have consequences in the real world. Some states have recently entered the fray and taken matters into their own hands, legislating against anonymity both in and out of cyber-space.

USA

The First Amendment to the United States Constitution reads in part that, "*Congress shall make no law . . . abridging the freedom of speech or of the press . . . designed to prevent the majority, through acts of Congress, from silencing those who would express unpopular or unconventional views*". The Amendment's purpose is to encourage formation of public forums into which messages may be inserted without censorship. Although most courts and commentators agree that protecting freedom of speech is important to fostering the marketplace of ideas, practitioners also recognize that the First Amendment does allow some regulation that may limit free speech. In other words, the Amendment does not guarantee individuals the right to say whatever they want without accountability.

Under the USA Patriot Act, Congress abolished these limitations in 2001, requiring simply that the records would be needed for foreign counter-intelligence purposes. Disclosure of documents-such as credit reports, bank records, and telephone/Internet billing and transaction records, and even access records to books in public libraries can be obtained when asked for by an FBI agent.

14 Jonathan D. Wallace -Nameless in Cyber-Space, Anonymity on the Internet

EUROPE

The Council of Europe has also made recommendations in this area (Recommendation No. R99) stated in its preamble that there is, *"a need to develop techniques which permit the anonymity of data subjects ... while respecting the rights and freedoms of others and the values of a democratic society.* The recommendation later suggests[15]", but does not expand upon, the fact that in some cases complete anonymity may not be appropriate because of legal and other constraints.

DENMARK

In March 2004 the Danish Ministry of Justice released a draft Administrative Order and a set of guidelines for the mandatory retention of telecommunication traffic data. It is a follow-up to the anti-terror package of June 2002 (Act 378) that extended the minimum time for data retention to a year, and allowed police and intelligence agents to look at such material with court permission where serious crimes were involved. ISP servers have to install software similar to the US system[16] to intercept e-mails.

The Loopholes

Privacy is a touchy subject for most people. The proposed legislative bills and the governmental policy studies on privacy show that Internet users and citizens demand more privacy protection. The problem lies in the fact that the Internet was created for the freedom of all users, and that includes the right to collect information about others. It is felt therefore that the purpose of the Internet may be best served as its own monitor in matters of privacy.

With the advent of cyber-space, communications have vastly increased on a global scale. High-speed communication at minimal cost, combined with ever-improving technology, has ushered in an era of easily accessible, truly anonymous communication. Unique new forms of pseudo-anonymous communication have also developed. Citizens and legislatures alike have responded to these changes with both well-founded and ill-founded beliefs and confusion. These beliefs have recently begun to clash, leading to showdowns in the real world, in cyber-space, and in courtrooms.

There are many different ways to communicate in cyber-space, and hence many ways to communicate anonymously. On one level of interaction, individuals can assume pseudonyms, enter virtual chat rooms, and converse with others on nearly any subject. On another level of interaction, individuals can create and view web pages. The identities of the people engaged in these forms of communication are not always easy to discover.

It is possible that new developments in technology may effectively eradicate some forms of truly anonymous communication. For example, the implementation of a new Internet protocol could improve the ability of law

15 http://www.lclark.edu/~loren/cyberlaw99/projects/kdavid/projhome.htm
16 http://www.sics.se/privacy/news-letters/nl-2004-08-05.txt

enforcement to track cyber-space communications through unique identifiers attached to every computer's IP number.

Although anonymous remailers constitute the bulk of truly anonymous communication in cyber-space, there are other ways to achieve true anonymity. Accounts on Internet email services, such as Hotmail.com are available to anyone upon request. Although these services ask for the user's name and address, this information is rarely verified. Therefore, any message sent is only traceable to the computer that sent it. Anyone accessing the Internet from a public terminal can keep his or her true identity a secret. Such public Internet connections are easy to find as many libraries and sidewalk cyber-cafes offer this type of access.

Despite the fact that anonymous messages can be sent without the use of an anonymous remailer, the latter pose the greatest problem for legal control[17]. Although anti-remailer legislation might shut down some poorly funded basement hackers, the world-wide nature of cyber-space allows dedicated truly anonymous remailers to function as advertised, because the remailer operators can avoid legislation by moving outside the jurisdiction.

Anonymity offers both advantages and disadvantages. For example, in countries where free speech is not protected by the authorities, hiding true identity becomes important, and can give the oppressed a voice. On the other hand, users can also hide behind anonymity to preach racial hatred or to share child pornography with complete impunity. The question then is one of deciding which one outweighs the other.

For anti-anonymity legislation to succeed, it must narrowly target specific evils. Governments must recognize that within the distinction between true anonymity and pseudo-anonymity lies the key to legislative restrictions. Because some types of anonymity, such as political speech, are considered valuable and necessary elements of society, legislation cannot merely target all true anonymity under the assumption that its existence promotes anonymous criminal acts. Legislatures must isolate and target only the specific type of anonymous speech in cyber-space which has criminal objectives, such as cyber-stalking or child pornography.

The Suggested Solution

To increase the effectiveness of this proposal, legislatures would have to take some additional steps. For example, legislation that forced email service providers to keep logs and verify the identities of their users, combined with legislation that forced local libraries and sidewalk cyber-cafes to register the identities of people using their computers, would decrease people's ability to send truly anonymous communication. There may even be an attractive alternative; instead of keeping records of sender names, remailers could simply

17 http://www.mttlr.org/volseven/du pont.html

allow the encrypted IP address of the message sender to pass through unmodified. This would enable message senders to comply with the anti-anonymity legislation while sending messages that are close to truly anonymous.

Because cyber-space enables truly anonymous communication to flourish on a scale never before experienced, its existence promotes anonymous criminal acts. As the influence of cyber-space increases in society, these acts will only become more prevalent. Although no one can stop a determined person from sending a truly anonymous electronic message, letter, or phone call, authorities can attempt to catch the criminals who do, and legislatures can take preventive action so that it does not happen again. Educated legislators can criminalize most true anonymity in cyber-space, as long as they provide viable and realistic alternatives for anonymous communication.

In order to stop the boom in criminal cyber-conduct and to prevent the anonymity of cyber-crimes, a future Law of Cyber-Space must criminalize the use of any kind of techniques which aim at concealing a person's true identity with the intentional scope of committing any kind of cyber-crime. The perpetrators should be punished at a level corresponding to the seriousness of the crime committed; the fact of concealing ones identity should be considered as an aggravating circumstance. The ideal would be to make such crimes an extraditable offence.

CHAPTER 04. DATA PROTECTION

The Problem

Of all the human rights in the international catalogue, privacy is perhaps the most difficult to define. Definitions of privacy vary widely according to context and environment. In many countries, the concept has been fused with data protection, which interprets privacy in terms of the management 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 an individual's personal affairs. The lack of a single definition should not imply that the issue lacks importance. As one writer observed, *"in one sense, all human rights are aspects of the right to privacy"*.[18]

Data protection also known as information privacy, involves the establishment of rules governing the collection and handling of personal data, including credit information, and medical and government records.

Data protection is not a new concept in itself, but has become an increasingly important issue in the digital age. Data protection has increasingly become part of the mainstream of the legal debate, in part due to the burgeoning growth of e-commerce. Data protection can be defined as safeguards to protect the integrity, privacy and security of data. The focal point of data protection is that of individual autonomy, or the ability of an individual to control access to his personal information. However, the collecting, collating, manipulating and use of personal data has become increasingly easy now for private companies.

The problem has been compounded by the measures that have been initiated to control and suppress acts of terrorism. While such measures are demonstrably necessary they must be proportionate with due regard to the human right to privacy.

There is an urgent need to develop minimum standards at international level to control the holding and use of personal data.

The safeguarding of information about individuals which is stored on computers would require computer databases containing personal information to be registered, and then to apply the following principles:

- fairly and lawfully process;
- processing for limited purposes;
- adequacy, relevance and absence of excessiveness;
- accuracy;
- no filing for longer than is necessary;
- processing in line with personal rights;

18 Lawrence T. Greenberg, Seymour E. Goodman, Kevin J. Soo Hoo, National Defense University Press1998

- security;
- no transfers to third parties without adequate protection.

The Existing Texts

Privacy is recognized around the world in diverse regions and cultures. It is protected in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and in many other international and regional human rights treaties. Nearly every country in the world includes the right of privacy in its constitution. At a minimum, these provisions include the right to inviolability of the home and to the secrecy of communications.

Other most recently written constitutions include specific rights to access and control one's personal information. In many of the countries where privacy is not explicitly recognized in the constitution, the courts have applied that right on the basis of other provisions. In many countries, international agreements that recognize privacy rights have evenbeen adopted into law.

The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, and the Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data, set out specific rules covering the handling of electronic data. These rules describe personal information as data that are afforded protection at every step from collection to storage and dissemination.

These two agreements have had a profound effect on the enactment of laws around the world. Nearly thirty countries have signed the CoE Convention and several others are planning to do so shortly. The OECD guidelines have also been widely used in national legislation, even outside the OECD member countries.

EUROPE

In 1995, the European Union enacted the Data Protection Directive in order to harmonize member states' laws in providing consistent levels of protections for citizens and ensuring the free flow of personal data within the European Union. The directive sets a baseline common level of privacy that not only reinforces current data protection law, but also establishes a range of new rights. It applies to the processing of personal information in electronic and manual files.

A key concept in the European data protection model is enforceability. Data subjects have rights established in explicit rules. Every European Union country has a data protection commissioner or agency that enforces the rules. It is expected that the countries with which Europe does business will need to provide a similar level of oversight and enforcement.

Under the EU Data Protection Directive, all European Union member states must have an independent enforcement body. These agencies are given

considerable power: governments must consult the body when the government draws up any legislation relating to the processing of personal information; these bodies also have the power to conduct investigations and have a right to access information relevant to their investigations, or to impose remedies such as ordering the destruction of information or ban processing, and start legal proceedings, hear complaints and issue reports.

The Directive imposes an obligation on member states to ensure that the personal information relating to European citizens has the same level of protection when it is exported to and processed in, countries outside the European Union. This requirement has resulted in growing pressure outside Europe for the passage of privacy laws. Those countries that refuse to adopt adequate privacy laws may find themselves unable to conduct certain types of information flows with Europe, particularly if these involve sensitive data.

In June 2002 the European Union Council adopted the new Privacy and Electronic Communications Directive. Under the terms of the new Directive, member states may now pass laws mandating the retention of the traffic and location data of all communications taking place over mobile phones, landline telephones, faxes, emails, chat rooms, the Internet, or any other electronic communication device. Such laws can be implemented for purposes ranging from national security to the prevention, investigation and prosecution of criminal offences.

USA

Privacy protection in the United States is based on an approach which is sectoral and self-regulatory approach[19]. In 1998, the United States began negotiating a Safe Harbor agreement with the European Union in order to ensure the continued transborder flows of personal data. The idea of the Safe Harbor was that United States companies would voluntarily adhere to a set of privacy principles worked out by the United States Department of Commerce and the Internal Market Directorate of the European Commission.

The principles of Safe Harbor Agreement signed in 2000, require all signatory organizations to provide individuals with clear and conspicuous notice of the kind of information they collect, the purposes for which it may be used, and any third parties to whom it may be disclosed. This notice must be given at the time of the collection of any personal information or as soon thereafter as is practicable. Individuals must be given the ability to choose (opt-out) the collection of data where the information is either going to be disclosed to a third party or used for an incompatible purpose. In the case of sensitive information, individuals must expressly consent (opt-in) to the collection. Organizations wishing to transfer data to a third party may do so if the third party subscribes to Safe Harbor or if that third party signs an agreement to protect the data. Organizations must take reasonable precautions to protect the

19 www.privacyinternational.org/ survey/phr2003/overview.htm

security of information against loss, misuse and unauthorized access, disclosure, alteration and destruction. Organizations must provide individuals with access to any personal information held about them, and with the opportunity to correct, amend, or delete that information where it is inaccurate. This right is to be granted only if the burden or expense of providing access would not be disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual would not be violated. In terms of enforcement, organizations must provide access to readily available and affordable independent recourse mechanisms that may investigate complaints and award damages. They must issue follow up compliance procedures and must adhere to sanctions for failing to comply with the principles.

APEC

In 2003, the 21 Asia-Pacific Economic Cooperation (APEC) economies commenced development of an Asia-Pacific privacy standard, and a subsequent procedure for handling data export limitation issues. This becomes the most significant international privacy initiative since the European Union's Data Protection Directive of the mid-1990s. In February 2003, Australia put forward a proposal for the development of APEC Privacy Principles, using the 1980 OECD Guidelines[20] on the Protection of Privacy and Transborder Flows of Personal Data as a starting point. A Privacy Sub Group was set up comprising Australia, Canada, China, Hong Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States. In March 2004, Version 9 of the APEC Privacy Principles was released as a public consultation draft. Implementation mechanisms, including mechanisms relating to trans-border data flows are still under consideration.

The positive side of the APEC privacy initiative is that it has the potential to encourage the development of stronger privacy laws in those APEC economies that provide little privacy protection at present, and to help find a regional balance between the protection of privacy and the economic benefits of trade involving personal data. The negative side is that it also presents considerable potential dangers to long-term regional privacy protection if it becomes a means by which the APEC economies accept lower standards. Globally, a high APEC standard could be a means of resolving international data export issues, but low APEC standards could entrench a privacy confrontation between Europe and the Asia-Pacific. The history to date of the APEC initiative shows that the dangers are as great as the potential benefits, but a valuable outcome for privacy protection is still possible.

The Loopholes

Potentially coercive powers for collecting evidence in the field of information technology cover both personal and non-personal data. With

20 http://www.anu.edu.au/people/Roger.Clarke/DV/PaperOECD.html

respect to personal data, however, there are legal problems that mainly concern gathering, storing and linking personal data in the course of criminal proceedings. In this field of privacy protection in criminal matters, legal requirements vary considerably among countries [21]. Differences between various legal systems are found not only in substantive legal requirements but also in the constitutional background, legal context and legislative technique of the relevant provisions.

Some of the problems related to procedural laws that may be difficult to overcome due to the differences between legal systems are as follows:

- Collecting data stored or processed in computer systems generally first requires entry into and search of the premises in which the computer system is installed; it is then necessary that the data can be seized or captured.
- The investigation of computer data permanently stored on a corporeal data carrier does not, in most countries, pose serious problems, since the right to seize and to inspect the corporeal data carrier or, in case of internal memories, the central processing unit, also includes the right to inspect the data. In other words, there is no difference whether the data is fixed with ink on paper or by magnetic impulses in electronic data carriers.
- The application of the traditional powers of search and seizure might, however, cause problems in cases where data are not permanently stored in a corporeal data carrier. In these instances, it is questionable whether pure data or information can be regarded as an object in the sense of criminal procedural law. The same holds true if the legal principle of minimum coercion or of proportionality makes it unlawful to seize comprehensive data carriers, or complete computer installations, in order to gather only a small amount of data. Similarly, the search and seizure of comprehensive data carriers could cause serious prejudice to business activities or infringe the privacy rights of third parties. Uncertainties may also arise in cases in which data carriers (such as core-storage, fixed-disk devices or chips) cannot be taken away to be evaluated on a police computer but must be analyzed using the computer system in question. In all these cases one might consider applying the powers of search not only to detect a computer installation and data but also to fix (especially to print) the relevant data on a separate data carrier and then seize this new object, which might be a diskette or a printout.
- Special problems also arise with respect to search and seizure in computer networks. Here, it is questionable whether and to what extent the right to search and seize a specific computer installation

21 Statement to the World Summit on the Information Society Nyon, 16-17 October 2002

includes the right to search databases that are accessible by this installation, but which are situated in other premises. This question is of great practical importance since perpetrators increasingly store their data in computer systems located elsewhere in order to hinder prosecution. Specific problems of public international law arise with respect to search and seizure of foreign databases via international telecommunication systems. In these international systems, the direct penetration by prosecuting authorities of foreign data banks generally constitutes an infringement of the sovereignty of the State of storage (and often in a punishable offence); however, there might be some specific exceptions that could be developed internationally in which direct access to foreign data banks via telecommunication networks could be permissible and the lengthy procedure of mutual assistance avoided.

- Problems of interpretation also arise with respect to extra safeguards for specific information. This is not only an issue with respect to the materials of professional legal advisers, doctors, journalists and other people who may, in some legal systems, be exempt from giving evidence. One of the latest disputes in this area is the question of how far the privileges of the press should also be applicable to electronic bulletin boards. Even more intricate questions arise with the application of safeguards and specific provisions normally associated with papers, documents and letters, to the new fields of electronic mail and telecommunication systems.

It is useful to draw attention to the fact that the law and policy on data privacy have tended to operate for regulatory purposes with a fairly clear distinction between data/information on the one hand, and the person to which the data/information can be linked, on the other hand.

The situation is now different, largely because of the developments that merge information and communication technology with biotechnology to create bioinformatics[22] and biometrics[23] in order to link data irrefutably with individuals.

The massive filtering of the Internet represents one of the most delicate issues. This is because filtering technologies are prone to two simple inherent flaws: under-blocking and over-blocking. While these technologies can be effective at blocking specific content such as high profile web sites, the technology cannot filter similarly categorized content that is spread out across multiple domains: websites, news groups, email lists, chat rooms and instant messaging.

22 Dr. Lee A. Bygrave, Reflections on the relationship of data privacy law with the human body.

23 S.D. Warren & L.D. Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review.

- Under-blocking refers to the fact that content filtering technologies are incapable of blocking all content deemed "*unacceptable*". With minimal effort restricted content can be traced and accessed. On the other hand, filtering technologies often block content that they do not intend to block. Many blacklists are generated through a combination of manually designated web-sites as well as automated searches. Thus web-sites are often wrongly classified and end up on blocking lists.
- Over-blocking is a significant challenge to the access to information on the Internet as it can put excessive control over access in the hands of private corporations and unaccountable governmental institutions. In addition, because the filters can be proprietary, there is no transparency in terms of the labeling and restricting of web-sites. The danger is most explicit when the corporations that produce content filtering technology work alongside undemocratic regimes in order to set-up nation-wide content filtering schemes. Most states that implement content filtering and blocking build customized blocking lists that sit on top of commercially developed technologies and blacklists.

The Suggested Solution

A lack of international coordination and cooperation can have detrimental effects on national and international economies, on trade, and on an individual's participation in the social, cultural and political life. The international understanding of and domestic implementation of measures that are required to enhance the security of information systems and facilitate the international exchange of data and commerce are important.

National boundaries, which may have hindered the activities of criminals in the past, have effectively, disappeared with the advent of modern telecommunications. In gathering evidence, investigators must be able to understand and deal with international issues. The laws of evidence, criminal procedure and data protection of other jurisdictions must be considered when pursuing international investigations. This will need a common approach relating to:

- the field of coercive powers;
- the legality of processing personal data in the course of criminal proceedings; and
- the admissibility of computer-generated evidence in court proceedings.

It is also worthwhile to mention that the dynamic nature of computer technology, compounded by specific considerations and complications in applying traditional laws to this new technology, dictate that the legal and judicial communities must develop new skills to be able to respond adequately

to the challenge presented by computer crime. The growing sophistication of telecommunications systems and the high level of expertise of many system operators, significantly complicate the task of regulatory and legal intervention.

In seeking solutions to the above problems, the international community should strive for maximizing cooperation between nations in order to address the potential for enormous economic losses and the general threat to privacy and other fundamental values, which cross-border electronic transactions may create. Worldwide protection must guarantee against havens, where computer criminals can find refuge or from where they can launch their attacks.

A structured scheme for international cooperation is needed, which takes into account and balances the necessities of international trade and relations, on the one hand, and the rights and freedoms of the individual, on the other hand.

CHAPTER 05. SOFTWARE, INCLUDING ENCRYPTION

The Problem

A software or computer program is a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result. The translation of data into a secret code, or encryption, is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.

Protecting copyright in software is an issue that attracts much attention. While much is made of the fact that an effective protection strategy needs to be both legal and technical, legal commentators frequently gloss over the detail of available technical protection strategies. Technical commentators assume a level of programming familiarity which a general audience may not, and frequently does not, possess.

Software piracy is the illegal use, duplication or distribution of a software product without the permission of its owner, violating copyrights or intellectual property rights. Current laws protecting software copyrights are based on the agreement on Trade-Related Aspects of Intellectual Property Rights[24] as part of the World Trade Organization agreements.

It is evident that these provisions have provided a firm legal basis for the protection of software copyrights within the software industry. In view of the proliferation of illegal copies of software available on the Internet, it appears however that legal protection alone might not be sufficient. The legal right to software protection does not provide complete power or control. The argument is well known. No one has a right to enter your house without your consent. The inviolability of your house is protected by law. Nevertheless, you prefer to have a lock in your door. Although software products are adequately protected by law, it is prudent to lock or protect software against piracy as computer software can be copied and distributed easily.

A new complication has been introduced by the misuse of the Internet as an enabling tool for acts of terrorism. This has led to restrictions on encryption technology. This is particularly true of high-end encryption techniques.

The Existing Texts

Software is a term which is much too broad to use in the application of copyright protection. Instead copyrights are applied separately to graphics or other design elements, site mapping, source and object code, algorithms, program or other technical descriptions, data flow charts, logic flow charts, user manuals, data structures, database contents, almost anything written. To apply copyright law the specific thing to be protected must be clearly identified. While copyright law protects against the literal copying of graphics or other

24 www.softwareprotection.com

designs, source or object code, text or documentation, the protection of the web site or program structure and other elements from non-literal copying may be more problematic.

Many have argued that patents, not copyrights, are now the only way to give adequate protection to the most important aspects of software[25]. This may be true because the idea behind a particular algorithm is much better protected as a patentable method, than as a narrowly limited expression in copyright law. Most software designers are interested in preventing others from stealing the core methodology used in their software. As such, a patent on the software could be obtained. The principal benefit of protecting computer software through a patent system lies in the strength of protection that is provided by a patent.

Around 93 countries of the world have implemented copyright laws, and about 60 of them have implemented patent laws[26]. They are also part of corresponding international treaties such as the Berne Convention, the Patent Cooperation Treaty, the Universal Copyright Convention, the Eurasian Patent Convention, the Paris Convention, the World Trade Organization and the European Patent Convention.

Copyright Laws criminalize the so-called software piracy, or the unauthorized use of software. Such copyright infringements include the illegal duplication of copyrighted software, or the installation of copyrighted software on more computers than authorized under terms of the software license agreement. When an individual or institution purchases software, they only purchase the right to use the software. The copyright belongs to the developers of the corporation which produces the software.

It is a truism that the advent of the Internet enables every user to easily become a potential pirate, empowered to disseminate an unlimited number of perfect digital copies to all the reaches of the globe. It is not surprising that copyright owners hesitate to introduce their most valuable products into that environment if the only legal control they can maintain is what is provided by national copyright laws, which may be difficult or costly to enforce in many jurisdictions. The fact is that some of these works will not be made available online except within the framework of a licensing regime that the copyright owner can reasonably conclude will be enforceable. To the extent that national laws discourage or weaken such regimes by limiting contractual freedom, the online digital marketplace in that nation may fall short of its full potential as a rich source of authorized works. Clearly legitimate users have a stake in a legal environment that encourages copyright owners to make full use of this uniquely powerful, yet uniquely risky, dissemination channel.

25 http://www.murdoch.edu.au/elaw/issues/v10n4/halbert104.html
26 www.uspto.gov/web/offices/ dcom/olia/diplconf/briefing.pdf

In the absence of a contract, the extent to which a customer may reproduce or make other uses of copyrighted[27] material is governed by statutory standards such as fair dealing (in Australia) or fair use (in the US), which are flexible by design in order to retain meaning in a changing world. A licensing structure offers the parties the opportunity to draw the line between permitted and excessive uses with much greater clarity. To the extent that a license agreement is able to define permitted uses more clearly at the outset, both parties can proceed with the transaction with greater predictability and with the confidence that their legitimate interests will be protected.

Licensing regimes facilitate making materials available on the precise terms that best meet the demands of a particular market. The advantages are obvious and widespread. A business needing only intermittent access to a specialized software application saves money in comparison to another business that needs it twenty-four hours a day, seven days a week. On the other side of the bargain, copyright owners are able to reach market niches that might be priced out of the market or missed altogether under the all or nothing outright sale paradigm. The result, once again, is greater access by a wider public than would otherwise be achievable.

The Loopholes

The problem could be viewed from two perspectives, namely, (a) that the very concept of copyright has never been of benefit to society in general, and has always served simply to enrich a few at the expense of the many; and (b) that the current copyright system does not work in the new information society.

There are also some who defend copyright as a concept to protect authors' rights, but feel that it outlives its welcome by granting protection for too long, often far beyond the lifetime of its owner.

To most critics, the general problem is that the current international copyright system undermines its own goal. The concepts of the public domain and of the intrinsic freedom of information are necessary precepts for creators to be able to build on works published elsewhere. But these are gradually being eroded, as copyright terms are repeatedly extended to last beyond the lifetime of the audience which knew of the original work.

One can of course argue that irrespective of contemporary advances in technology, copyright remains the fundamental way by which authors, sculptors, artists, musicians and others can fund the creation of new works, and that absent legal protection, many valuable books and pieces of art would not be created. This interest is arguably served even by repeated extension of copyright terms to encompass multiple generations beyond the copyright holder's life, not only because many authors and copyright holders are

27 http://www.himels-computer-law.com/copr.htm

corporations, but also because the right of an author's heirs to continue to profit from a protected work may provide a substantial part of the incentive to create.

One counter-argument to this, however, is the recent success of free software projects. These popular products have demonstrated that quality works can be created, even in the absence of copyright-enforced monopoly rents. It should be noted, however, that these products still use copyright in order to enforce their license terms, even if those licenses are not for monetary gain.

Copyrighted works replicated onto digital media are easily and trivially copied via file sharing, and those who do this routinely break copyright laws hundreds or thousands of times, typically with minimal thought or concern. Attempts to prevent this have been largely unsuccessful, and file sharing almost never results in severe consequences for the violators. While producers of copyrighted material often attribute losses in their sales to online copying, yet they generally continue to produce material and to make profits. This lack of apparent effect has been gradually eroding the belief that copyright is indispensable.

A few artists actually support the file sharing of their own works, arguing that it expands their audience to include people who would not otherwise be able or willing, to legally purchase their material.

The Suggested Solution

The primary purpose of any recommendation would be to harmonize laws globally and to create a single universal statute. There are ambiguities and inconsistencies in the right of reproduction, on communication to the public, and on exceptions to copyright. A good example is set out in the WIPO Copyright Treaty (WCT) of 1996, which aims to protect computer programs by copyright. Even though there are 54 Contracting Parties to this Treaty, and even though the Convention of Cyber-crime of European Union refers to the Treaty and provides for the penal sanctions, this is still a regional regulation. What is needed is a single global framework to cover the problem in its entirety.

Therefore there is a great need to agree upon criminalizing the duplication or distribution of a software product without the permission of its owner, in violation of the copyrights or the intellectual property rights. In order to attribute the proper penalties for this crime, states should implement identical provisions at their domestic level, and use international cooperation mechanisms effectively.

CHAPTER 06. MALICIOUS CODE

The Problem

As the Internet has grown into a graphical, multi-media user experience, programmers have created scripted languages and new application technologies. As with any new technology, programs written with scripted languages run the gamut from useful, to poorly crafted, to outright dangerous[28].

Technologies such as Java enable all such programs to be executed on user workstations. The web increases the mobility of code without differentiating between program quality, integrity, or reliability. Using available tools, it is quite simple to drag and drop code into documents that are subsequently placed on web servers and made available to employees throughout the organization, or to individuals across the Internet. If this code is maliciously programmed, or just improperly tested, it can cause serious damage.

Malicious code refers to a broad category of software threats to your networks and computer systems. Perhaps the most sophisticated types of threats to computer systems are presented by malicious codes that exploit vulnerabilities in these systems. Any code which modifies or destroys data, steals data, allows unauthorized access exploits or damage a system, and does something that a user did not desire, is called malicious code.

The most common type of malicious code is a *Virus*. It can infect systems by attaching itself to files and programs. Just like its biological counterpart, it needs a host to infect. A virus is usually a program that needs to be executed by a user before it can do any damage. For example, a virus attached to an email message is usually harmful only when a user opens or executes the attachment.

A *Worm* is similar to a virus but with one main important difference: a worm does not need to attach itself to a file or program to be reproduced and executed as in the case of a virus. A worm is self-contained; it can replicate itself and infect entire networks. Most worms can be easily removed from a system by using a decent anti-virus utility.

Trojan Horses and *Back Doors* are higher level tools for the more serious attacker. They are often used in conjunction to allow the attacker to gain remote control of the target system and/or steal information. A Trojan horse is a seemingly harmless piece of software that contains malicious code concealed within its own. The malicious code is typically a back door, also known as an illicit server, but it can be a virus, worm or any other kind of code that allows the attacker to do damage.

A *Logic Bomb* is a smart piece of malicious code that executes only when certain conditions are met. For example, an attacker could implement a logic

28 www.finjan.com/SecurityLab/KnowledgeCenter/ CurrentTopics/ActiveContentandMaliciousMobileCode.asp

bomb on a public Internet client that will start only when a user types in user credentials at a website. Other examples are a virus that executes on a particular date, but whih had infected the system long before that date. In other words, a logic bomb contains a mechanism that is triggered only when a certain event occurs, say on a particular date, or when activated by a certain trigger action.

The Existing Texts

EUROPE

The aim of the EU Convention on Cyber-crime is to provide computer data and computer programs with protections similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest is the integrity and the proper functioning or use of stored computer data or computer programs.

The deletion of data is the equivalent of the destruction of a corporeal thing. It destroys or makes data unrecognizable. The suppression of computer data is defined as any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term alteration is defined as the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data.

USA

Causing damage to national computer networks is a federal crime, one that carries substantial penalties for those convicted. The principal federal law in the battle against computer viruses and worms is the Computer Fraud and Abuse Act, 18 USC. 1030.

Section 1030 - Fraud and related activity in connection with computers:

a) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

b) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

c) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage.

The Loopholes

Privacy laws are a patchwork quilt of state and federal laws, rules, and regulations that have numerous loopholes.

There are many who take the view that the existing legislation already covers denial of service attacks without any need for amendments, and that the better preparation of cases and more sophisticated evidence gathering

techniques, rather than legislative change, hold the key to combating the rising wave of cyber-crime.

The digital world presents a fast-changing environment with many unfamiliar aspects. It places particular challenges onto legal systems, which find it difficult to cope with the rate of change of this new world. Technical innovation continues at breakneck speed, people (including criminals) make innovative use of its capabilities; geographic boundaries become less well defined (creating jurisdictional problems). If the growth in e-crime is to be contained, we need laws to become better adapted to this new environment.

Whether existing laws are amended, or new laws created, two further issues need to be considered. The digital world has the potential to enable ever greater intrusion on, and control of, members of society by government[29]. It is also a highly complex technical world under constant change. The need is for laws and regulations to be written in ways that are technically neutral, thus reducing the need for continuous amendment as technology evolves, mutually consistent and sufficiently well defined to maintain an acceptable balance between the needs of the state to protect society, the freedom of the individual and the ability of organizations to take reasonable steps to reduce risk. As part of this process, industry should contribute more directly to supporting the investigation and prosecution of e-crime, working to the same standards as, and with, law enforcement. This will require changes to current laws and regulations, although the extent of these changes is far from clear at this time.

The Suggested Solution

There are many legal issues associated with the drive to reduce cyber-crime as it is related to malicious code. Three key actions need to be initiated now to create a sound legal environment:

- There is an urgent need to agree on priority changes and to schedule them into the legislative process at the earliest opportunity.
- As part of this process, the responsibilities and liabilities of those whose systems are used for criminal activities need to be clear and understood, with an acceptable balance between intrusion and privacy. This will require that existing laws and regulations be re-visited.
- International jurisdiction issues being addressed by governments need to be supported by those in industry.

The immediate need is to facilitate low overhead co-operation at the start of the investigation when the location of those causing the problem is still unclear. Governments must work with the private sector in ensuring that those with front-line experience and responsibility contribute directly to the development of practical solutions.

29 www.eurim.org/consult/e-crime/ dec03/ECS_WP6_web_031209.htm

They should strive to criminalize the use of software codes which modify or destroy data, the stealing of data, the unauthorized access, and the exploitation or the damage to a system. This kind of criminal conduct must be punished with fines and imprisonment but for this to become reality, states need to implement identical provisions at their domestic levels.

CHAPTER 07. SPAM

The Problem

Unsolicited commercial communications or *spam*, as it is more usually known, has grown into one of the major plagues affecting today's digital world. In a very short period of time, spam has become more prevalent than legitimate e-mail correspondence. Spammers are now sending hundreds of millions of messages every day, causing significant financial costs and losses in productivity for service providers, businesses and e-users.

With the growing dependence of users on e-mail for their personal and professional communications, spam can seriously hamper the development of the digital economy and society by undermining users' confidence in online activities. These problems have hit epidemic proportions.

Spam is the most pernicious and irritating aspect of modern life, a phenomenon that costs businesses worldwide billions of dollars each year, projected to continue to escalate at an astounding rate.

Spam is unsolicited commercial e-mail (UCE), unsolicited bulk e-mail (UBE), gray mail and just plain junk mail. It is used to advertise products or to broadcast some political or social commentary. The term was applied for the first time to articles posted to online message boards, which were of no relevance to their discussions and violated their forum policies. Such articles were sent to several newsgroups, and quickly became a nuisance to other users. The term was then applied to describe junk e-mail messages, usually advertisements for products and services. In determining whether unsolicited e-mail is, or is not, a crime, the source and the motive must be considered. To qualify as spam the source must be intrusive (sent deliberately to many addresses) and without giving the recipients any option to "unsubscribe".

Everybody is agreed that a significant amount of spam involves fraudulent or deceptive messages. A clear distinction must be drawn between spam and legitimate commercial e-mail. One trend argued that spam is untargeted and unwanted e-mail which offers recipients no valid means to opt-in or opt-out. But legitimate commercial e-mail on the other hand respects the opt-in (receive no ads unless requested) or opt-out (receive all ads until individually declined) rights of recipients depending on the country they operate in.

Several stakeholders have given definitions of spam, and although there are many common points[30], there is still no universally accepted definition. Broadly speaking, spam includes all electronic messages that are unsolicited or unwanted, sent to a large number of users (bulk) without regard to the identity of the individual user, usually having commercial purposes, but which can also include viruses.

30 www.itu.int/.../spam/contributions/Background%20Paper_Building%20frameworks%20for%20Intl%20Cooperation.pdf

Spam activities are now spreading to mobile phone multi-media messaging and instant messaging services. The combination of mobile phones and Internet (such as the third-generation mobile services and wireless Internet) raises a host of possibilities for innovative applications and new modes of interaction. However, these opportunities have also been promptly spotted by spammers, who have begun to target mobile users. Considering that the number of mobile users worldwide has passed one billion, outnumbering fixed-line subscribers and making mobile the dominant communication technology of today, it is easy to imagine the potential impact of spam on mobile devices.

As the so-called third generation of wireless networks emerges, wireless advertisement, in the form of emails delivered to cellular phones is liable to explode. While this has the potential to provide attractive services to users and open the way for online mobile commerce, it is also likely to raise privacy concerns, to affect efficiency and reliability of services, and to diminish consumer trust. Spam is one of the most visible Internet threats, having grown at an explosive rate of 61% just in one year.

Like viruses, spam has become a scourge on the Internet as hundreds of millions of unwanted messages are transmitted daily to almost every email recipient as well as to newsgroups. Unfortunately for users and fortunately for spammers, as an advertising medium, spam does produce results. Even if only an infinitesimal number of users reply, it is still cost effective since e-mail is a very inexpensive way to reach people. It is simple mathematics: It may take only half an hour to send out a million messages, and supposing that out of every 1,000 of these spam messages only one person clicks the link and the spammer makes a dollar, the spammer will have made $1,000 in just that half hour. The entire job might not have taken more than a half hour for its set up.

As spam filtering becomes more sophisticated, spammers have to send even more spam to make the same money, but e-mail lists can be purchased for very little or hijacked, and there is a thriving ancillary business selling lists to spammers. There are even third-party spam service providers that will do all the work for you.

If spam makes up well over half of e-mail transmissions, then this translates into a massive data storage requirements. Information security systems are designed to preserve the integrity, the availability and the confidentiality of information processing resources and the data that they store or transmit. Since spam clogs up transmission, storage and computer processing, it presents a challenge to the availability of the systems for other legitimate users.

The Existing Texts

The legal framework that has been put in place in order to fight spam is complex, in particular due to the multitude of different laws that have been enacted in recent years, and the number of national authorities that are dealing

with this topic. The legal definition of what constitutes illegal spam varies depending on jurisdiction. The severest incrimination of spam is in the legislation of the United States, which set the punishment for this kind of offense as a fine, imprisonment up to 5 years, or both.

Anti-spam laws vary considerably in their approach to tackling the problem. However, unsolicited commercial e-mails are generally considered illegal when they conceal the sender's identity for example with the falsification of the point of origin and transmission path of unsolicited e-mail advertisements, or use a third party's domain name without consent, or provide misleading information on the subject line.

Also, for e-mail to be legitimate, many anti-spam legal instruments require:

- the prior authorization of the recipient (opt-in approach) or the existence of a prior business relationship before the sending of any commercial e-mail (soft opt-in approach). In some countries, where this approach is considered too severe, unsolicited emails, in themselves, are not considered illegal, but they must allow a recipient to no longer receive commercial communications from a certain sender (opt-out approach);
- a clear indication of the true name, geographical location and e-mail address of the sender;
- a procedure for address gathering which respects the right of privacy in the processing of personal data in the electronic communication sector;
- in some countries, the use of a label to warn about the content of a message.

AUSTRALIA

The Spam Act and associated Spam (Consequential Amendments) Act were passed by Parliament in 2003. The two Acts came into effect in April 2004, and are due for review within two years. Legislation will be administered by the Australian Communications Authority (ACA)[31]. In addition to a set of industry codes and standards, under the Spam Act, ACA[32] has the ability to pursue a number of enforcement options. As part of the changes, The National Office for the Information Economy becomes the Australian Government Information Management Office, with some functions transferring to the Department of Communications, Information Technology and the Arts' Information Economy branch. The regime of the Australian law regarding spam is Opt-in Laws.

CANADA

The Privacy Commissioner of Canada is an Officer of Parliament who reports directly to the House of Commons and the Senate as an advocate for

31 The Australian Communications Authority - The Spam Act's "Watchdog"
32 https://www.aca.gov.au/secure/complaint_form.htm

the privacy rights of Canadians. In May 2004, the Economic Development Agency of Canada for the Regions of Quebec, launched an Anti-Spam Action Plan and announced the creation of a ministerial task with Electronic Commerce Branch of Industry Canada to combat spam. Privacy Act 1980-81-82-83, c. 111, Sch. II *1*: The aim of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves which is held by a government institution, and which provides individuals with a right of access to that information.

EUROPEAN UNION

The European Commission (EC) has the following five directives that are relevant in regulating Spam, all of which include an "opt-in" regime:

- E-Privacy Directive: Directive 2002/58/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201).
- E-Commerce Directive: Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in Particular Electronic Commerce, in the Internal Market, 2000 O.J. (L 178) 1.
- Telecommunications Privacy Directive: Directive 97/66/EC Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector, 1998 O.J. (L 024) 1 (repealed and replaced by Directive 2002/58/EC).
- Distance Contracts Directive: Directive 97/7/EC on the Protection of Consumers in Respect of Data Protection Directive: Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31.

JAPAN

The basic document is the Law for Appropriate Transmission of Specified Emails (Law No.26 of 2002). In April 2002, the Japanese government also passed the Law on Regulation of Transmission of Specified Electronic Mail. This law addresses Specified Electronic Mail, which is defined as e-mail for advertisement purposes sent to users who have not opted in for the service. The law controls spam disseminated by anyone under the jurisdiction of the Ministry of Public Management, Home, Affairs, Posts and Telecommunications (MPHPT), which includes the entire country and the solitary islands. In July 2002 MPHPT established a body Japan Data Communications Association to determine the appropriateness of sending specified e-mail messages. The regime of the law is "opt- out".

IRELAND

The basic document is the Data Protection Act, 1988, EC Directive on Privacy and Electronic Communications, Directive 2002/58/EC[33], Statutory

33 http://www.oasis.gov.ie/utilities/redirect.php?url=http://www.dataprivacy.ie

Instrument, S.I. No. 535 of 2003, European Communities (Electronic Communications networks and Services) (Data Protection and Privacy) Regulations 2003 and The Data Protection Commissioner.

The Irish Government has formally signed a law outlawing spam. The law gives effect to new EU regulations banning the sending of unsolicited e-mails or text messages to the general public. Ireland passed the self-titled European Communities (Electronic Communications Networks and Services) (Data Protection and Privacy) Regulations 2003. Regulation 13 is about spam, and it starts strong with mandatory opt-in for unsolicited spamming. Regulation 19 grants enforcement powers to the Commission for Communications Regulation. The Regulator, in consultation with the Data Protection Commissioner, may also specify the form and any other requirements regarding the obtaining, recording and rescinding the consent of subscribers for the purposes of these Regulations. The punishment granted to the Commission is a warning. The regime of the law is "opt-in".

NEW ZEALAND

The Office of the Privacy Commissioner is an independent Crown entity established by the Privacy Act. The Government has issued a discussion paper to outlaw unwanted spam. The Privacy Commissioner's principal powers and functions include promoting the objects of the Privacy Act 1993[34], monitoring proposed legislation and government policies, dealing with complaints at first instance, approving and issuing codes of practice and authorizing special exemptions from the information privacy principles, and reviewing public sector information matching programs.

REPUBLIC OF KOREA

The basic document is the Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection of 2001[35]

Korea Spam Response Center was constituted within the KISA (Korea Information Security Agency), an agency of the Ministry of Information and Communication with the specific authority to deal with problems regarding spam. The regime of the law is "opt- out".

USA

In January 2004, the Can-Spam Act, which stands for *Controlling the Assault of Non-Solicited Pornography and Marketing Act*-117 Stat. 2699 Public Law 108-187, came into effect in the United States-Dec. 16, 2003.[36] This law puts specific requirements on senders of commercial e-mail and places enforcement in the hands of the Federal Trade Commission and State Attorney's General. The regime of this law is "opt-out".

34 http://www.med.govt.nz/pbt/infotech/spam/discussion/discussion-05.html

35 http://www.spamcop.or.kr/eng/m_1.html

36 http://www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm

UK

The UK's anti-spam law, the Privacy and Electronic Communications Regulations, came into effect. Many have said that this changes the standard for consumer e-mail marketing in the UK from opt-out to opt-in, but that is not strictly true. Confusion has arisen because legally there is a difference between the term consent, which is what the law actually requires, and opt-in, which is what everyone seems to think the law requires. In fact, the rules are not as restrictive as some have suggested.

The Loopholes

Governments are now becoming more involved in the matter, as they increasingly recognize the necessity of developing and applying such standards and of ensuring that they are internationally accepted. Although it would appear that technical solutions to spam and the problems of jurisdiction and enforcement in the Internet environment are unconnected, national and international regulation of technical measures adopted to limit spam may prove to be one of the most efficient method to control spam.

The use of labels[37] for e-mails having a specific content is a requirement in several countries. Often this condition is imposed only for messages having a sexually explicit content, to warn the recipient about the content of the e-mail, and in particular to avoid spamming children, who are often the unintended recipients of adult spam. Labels for commercial messages have also been imposed in countries such as the Republic of Korea. The use of a specific tag in the subject line of an e-mail allows users to identify commercial messages more easily, to set their filters by redirecting the messages to a specific folder, or to avoid their children receiving e-mail messages with pornographic content. The problem is that the rule is difficult to enforce in respect of anonymous spammers. But the problem arises even in the case of legitimate marketers who operate within the law. These labels are decided at the national level and vary from country to country, leaving the way open to messages originating from another country that does not use the same labeling system, causing an inevitable lack of uniformity.

Much debate has surrounded the adoption of the opt-in approach for spam messages in Europe[38]. Opt-in was considered as potentially threatening to the development of e-commerce and the Internet. What the opt-in/opt-out framework tries to achieve however, is not to outlaw direct marketing altogether, but simply to establish a fair and clear environment for legitimate marketing that is permission-based, while also reducing unwanted spam. The data must be collected fairly and used for specified, explicit and legitimate purposes. Yet this rule foresees an exception to its opt-in approach, allowing the sending of unsolicited commercial messages to users with whom the sender

37 www.itu.int/.../spam/contributions

38 www.itu.int/ni.

has a pre-existing business relationship. This exception, however, is applicable only for the advertisement of similar products and services, and for addresses used by the same person who legally collected the original data (opt-in). A further exception arises when the recipient is not a physical person but a legal entity. This exception is, however, subject to criticism, as business-to-business spam could have the same nature as spam sent to private users. In many countries, marketing companies are allowed to send messages to users without the need for prior authorization or relation, provided explicit opt-out language is included in every message. This can actually contribute to legitimate spam. Most users however, already have strong preconceptions regarding spam, and have been widely advised not to open or reply to any spam messages, to avoid sending out a confirmation that the e-mail address is active.

The jurisdictional problems created by the proliferation of trans-border unsolicited commercial communications represent what may prove to be an insurmountable hurdle. As spam touches on so many aspects of the law, such as commerce, advertising, criminal law, freedom of speech, and intellectual property, the differences associated with the laws of the jurisdictions of the world may prove greater than their similarities.

Moreover, self-regulatory approaches have a number of shortcomings, and technical solutions to date are only partially successful. A coordinated legal and technical approach, harmonized at the international level, would constitute a particularly promising approach. Although it is beyond the realms of possibility that spam will not exist anymore, if all players were to be proactive rather than simply reactive, unsolicited commercial e-mail could be effectively tackled.

On the technology front, the industry seems to be coalescing around the idea of adding sender authentication to email, letting recipients verify the source of a message. By verifying the sender's message address or the domain from which a message was sent, we would close the loophole left open by anonymous email.

The Suggested Solution

While opinions differ on the best way to cut down on abuse, everyone seems to agree it will take a combination of new technology, strong legislation, vigorous law enforcement, end-user education and international coordination to fight the problem.

The law generally regulates individual behavior by threatening *ex post facto* sanctions. However, in real space as well as cyber-space, this law also regulates individual behavior indirectly, by aiming to change markets, norms or code. It has been argued that law in cyber-space will often be more effective if it regulates code or architecture rather than trying to directly regulate individual behavior *ex poste facto.*

As the Internet has been developed by technologists and the private sector, both play an essential role in the long-term evolution of Internet architecture,

and must participate in the debate at national and international levels, so that their views can influence the creation of new solutions to combat the problem of spam.

Although there is no silver bullet that will eliminate spam entirely, the incidence of spam can be reduced and controlled. In general, it is widely recognized that the most effective solution to spam will combine legal and technological elements.

The crime of sending unsolicited e-mails or spam should be treated by all domestic penal laws as a criminal offense, and punished with fines and possible imprisonment.

CHAPTER 08. CYBER-HOOLIGANISM

The Problem

The Internet has evolved from a scientific and military network to a crime scene. The network is used by scientists, spies and terrorists alike. Even though the cost of attacks in cyber-space is rising at a fast rate, the network is so widely used that it cannot be possibly shut down. This opens the door then to a group of individuals described as *cyber-hooligans.*

Cyber-hooliganism is defined as a computer network related mischief such as defacing websites or releasing a virus or worm, without causing serious disruptions for the general population, or without creating widespread panic or terror. In addition to using computers for digital vandalism and low-level destruction. Another aspect is *hacktivism*, or using those tools to get a political message across.

Cyber-vandalism, or cyber-hooliganism, might include the knocking out of an e-mail system, defacing a Web site, or performing some other disruptive or annoying activity. Hackers seek to infiltrate secure computer systems in order to steal confidential information, such as the credit card data of customers.

Cyber-hooliganism is essentially non-violent, but can cause financial losses. For example, the creation of the *I Love You* virus or the destruction of the NASA web page were both cyber-hooliganism acts[39].

The Existing Texts

The Council of Europe Convention on Cyber-crime is the only attempt to regulate this kind of computer related crime. It defined the cyber-hooliganism as an offence against the confidentiality, integrity and availability of computer data and systems. The penalty for this kind of offence is left to different national legislations.

The provision aims at criminalizing the intentional hindering of the lawful use of computer systems including telecommunications facilities by influencing computer data. The term hindering refers to actions that interfere with the proper functioning of the computer system. Such hindering must take place by inputting, transmitting, damaging, deleting, altering or suppressing computer data. The hindering must furthermore be serious in order to give rise to criminal sanctions.

The definition of "serious" is understood to cover the sending of data to a particular system in such a form, size or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems, for example, by means of programs that generate denial of service attacks, malicious codes such as viruses that prevent or substantially slow the operation of the system, or programs that send huge

39 honey.7thguard.net/essays/cyberterrorism-policy.pdf

quantities of electronic mail to a recipient in order to block the communications functions of the system.

The "hindering" must be unauthorised. Common activities inherent in the design of networks, or common operational or commercial practices are considered as authorised. These include, for example, the testing of the security of a computer system, or its protection, as authorized by its owner or operator, or the reconfiguration of a computer's operating system that takes place when the operator of a system installs new software that disables similar, previously installed programs. Therefore, such conduct is not criminalized even if it causes serious hindering.

Nevertheless, Parties may have different approaches to. The text leaves it to the Parties to determine the extent to which the functioning of the system should be hindered, partially or totally, temporarily or permanently, before it reaches the threshold of harm that justifies sanction under law.

The most important aspect is that the offence must be committed intentionally, that is to say, the perpetrator must have the deliberate intent to seriously hinder.

The Loopholes

The open and defiant manner in which attackers currently operate reflects the weakness of the legal, defensive, and investigative capacities of the current system. Some attackers are snared after long, expensive investigations, but most go unpunished. This stems ultimately from the fact that the information infrastructure is transnational in nature. Attackers deliberately fashion their efforts to exploit the absence of internationally agreed standards of behavior and cooperation. For example, attackers can avoid prosecution or greatly complicate investigations simply by initiating attack packets from countries with inadequate laws, and routing them through countries that with different laws and practices, and no structures for cooperation.

The measures thus far adopted by the private and public sectors have not provided an adequate level of security[40]. While new methods of attack have been accurately predicted by experts, and some large attacks have been detected in early stages, the efforts to prevent or deter them have been largely unsuccessful, with increasingly damaging consequences. Intelligence exchanges have been slow, and investigations even slower. Some attacks are from states that lack adequate laws governing deliberate destructive conduct. A significant enhancement of defensive capabilities seems essential.

Cyber-crimes are often committed quietly, and remain unpublicised. According to the FBI, between 85% and 97% of crimes[41] are not even reported or revealed.

40 Sonia K. Katyal, Privacy Vs. Piracy, International Journal of Communications Law & Policy, Issue 9, Special Issue on Cyber-crime, Winter 2004/2005,

41 www.crime-research.org/articles/sabad03_2004/

The Suggested Solution

International laws must be drafted with the goal of securing speedy agreement among nations to adopt uniform definitions of offenses and commitments, despite having different network capabilities and different political interests[42].

The international community must encourage a universal recognition of basic offenses in cyber-space and the need for universal agreements to cooperate in investigating, extraditing, and prosecuting perpetrators. The law should describe the conduct it covers, including: interfering with the function of a cyber-system, cyber-trespass, tampering with authentication systems, interfering with data, trafficking in illegal cyber-tools, using cyber-systems to further offenses specified in certain other treaties, and targeting critical infrastructures.

The lack of an adequate international response to these weaknesses is puzzling, given the huge and growing financial impact of cyber-attacks and crimes. Even if some estimates of damages are inflated, the problem is becoming undeniably expensive to businesses, governments, and individual users around the world. Multilateral action is therefore required to build security into the underlying technical and social architecture. History has shown that when nations agree upon a common malicious threat, be it piracy on the high seas centuries ago, or aviation terrorism in the 20th century, a cooperative treaty mediated regime can contribute substantially to addressing the problem.

It is through such a treaty that cyber-hooliganism must be criminalized, because it presents a real threat in its ability to disrupt and to produce serious damages to computer networks. Such criminalisation would not be effective unless it is punished with fines and imprisonment; hence the need for punitive measures to complete the chain of the global legal system of regulation and implementation.

42 Abraham D. Sofaer, Seymour E. Goodman, A Proposal for an International Convention on Cyber Crime and Terrorism, 2000

CHAPTER 09. CYBER-STALKING

The Problem

With the popularity of the Web increasing each day, the act of stalking has now moved into the virtual realm of the Internet, and has come to be known as *cyber-stalking*[43]. Today, cyber-stalking is easier than ever, considering the anonymity provided by electronic communication. On the Web, it is not difficult to conceal one's identity or to provide incorrect personal information. Websites, e-mail, chat rooms, and discussion forums provide stalkers with a variety of opportunities to harass others. They also offer stalkers access to the private information of their victims.

While there is no universal definition for cyber-stalking, it is generally defined as stalking or harassing another person using the Internet, e-mail or other electronic communication devices. The Internet has all the anonymous features that stalkers love. With the simple push of a button, a stalker can send annoying or threatening messages to the victim's e-mail or post a message to a chat room or bulletin board. The Internet makes it easier for a shy stalker who might not want to call or physically follow a victim, but who has no problem sending a message through the Internet. Although a message received via the Internet seems harmless and less frightening, it can evolve into a more dangerous situation. As with physical stalking, cyber-stalking can ultimately lead to face-to-face confrontation and worse[44].

There are not many laws on the books to help the victims of cyber-stalking. Cyber-stalking is not yet a crime, and law enforcement agencies are limited to telling the victim to stay off their computers. As cyber-stalking can lead to more, so just turning off the computer is not very helpful. The resulting outcome of cyber-stalking can be devastating and it is for that reason that governments and states are trying to enact new laws and create new agencies to stop cyber-stalking and to protect citizenry.

Cyber-stalking can be divided into direct and indirect aspects.

- Direct cyber-stalking include: threats, bullying, or intimidating messages sent directly to the victim via e-mail or other Internet communications mediums, and/or the use of technological means to interfere with a victim's use of the Internet, such as hacking or denial of services attacks.
- Indirect cyber-stalking includes, but is not limited to, spreading rumors about the victim in various Internet discussion forums, subscribing the victim to unwanted online services, posting information about the victim in online dating or sex services, or sending messages to others in the victim's name.

43 http://en.wikipedia.org/wiki/Cyberstalking
44 www.ncjrs.org/pdffiles1/ojp/186157.pdf

The Existing Texts

Though stalking has existed for centuries, the legal system has only codified its presence in the statutes in recent decades. As a result, cyber-stalking could truly be identified as a crime of the 21st century owing to its reliance on computer and communications technology.

In legal terms, the manifestation of this misconduct is most likely to be charged as per the statutes in place in the respective jurisdictions. The incrimination of cyber-stalking varies greatly from misdemeanor[45] to serious crime. The penalties also are very different, starting from fines, peace bonds, restraining orders, protection orders up to 10 years imprisonment.

USA

In the United States,[46] California was the first state to adopt stalking laws, most often identified as a result of the murder of actress Rebecca Schaeffer by Robert Bardo in 1989. Legislation was subsequently passed in 1990. Until this passage of legislation the police was powerless to act unless the target was actually attacked physically. In 1998 the delict description was, "*Any person who willfully, maliciously, and repeatedly follows or harasses another person and who makes a credible threat with the intent to place that person in reasonable fear of his or her safety, or the safety of his or her immediately family, is guilty of the crime stalking*". Since then, almost every state in the USA has passed legislation making stalking a criminal offense[47].

AUSTRALIA

Australian[48] states which have enacted anti-stalking legislation around the same time include Queensland with Section 359A of the 1993 Criminal Code prohibiting unlawful stalking. Given the ability of individuals to mask their identity when using the Internet, linking the harassment to one particular individual may prove difficult. Programs that mask ones IP (Internet Protocol) address and anonymous remailers are merely two examples that hinder the identification of the digital location from which communications originate. Elements of the offense cover activities which could include such activities as: keeping a person under surveillance, interfering with property in the possession of the other person, giving or sending offensive material, telephoning or otherwise contacting a person in a manner that could reasonably be expected to arouse apprehension or fear in the other person, or engaging in conduct amounting to intimidation, harassment, or molestation of the other person.

UK

The Protection from Harassment Act[49] of United Kingdom came into force in June 1997 and was updated in August 2001. This Act makes provision

45 http://www.cyberlawenforcement.org
46 US Federal Laws on Cyberstalking
47 http://www.wiredpatrol.org/stalking/federal.html
48 http://www.aic.gov.au
49 HMSO Website.)

for protecting persons from harassment and similar conduct. In this sense a person must not pursue a course of conduct which can amount to the harassment of another.

CANADA

In Canada[50], the crimes of harassment and stalking, both on-line and off-line, are covered by the charge of Criminal Harassment, section 264 of the Criminal:

No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them. The conduct consists of:

a) repeatedly following from place to place the other person or anyone known to them;

b) repeatedly communicating with, either directly or indirectly, the other person or anyone known to them besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or

d) engaging in threatening conduct directed at the other person or any member of their family.

NEW ZEALAND

New Zealand Harassment Act 1997[51] states that:

a) harassment-cyber-stalking is a pattern of behavior that includes doing any specified act directed against that person on 2 separate occasions within 12 month period (may not be the same person as long as the pattern is directed against the same person).

b)specified Act means watching, loitering, preventing, following, making contact (whether by telephone, correspondence or any other way), giving, leaving, bringing attention to any offence material, entering, interfering with property, that would cause a reasonable person to fear for his/her safety.

THE NETHERLANDS

The violation of the privacy is regarded as an element of crime, and the police can in principle intervene early, even before the threatening actually begins. The Dutch definition of the offence does not imply the restriction that the victim must be clearly damaged by the actions of the offender. In July 2000 article 285b of the Criminal Code has become effective. With this article the penalization of stalking is provided for: *"He, who illegally and systematically infringes on someone else's privacy with the intention to force the other to do something, not to do or to endure, or terrify someone, will be punished, if guilty of stalking, with an imprisonment of at the most three years or a fine of the fourth category (25.000 Dutch guilders). Prosecution will only take place after a complaint of the person against whom a crime has been committed".*

The Loopholes

There is a definite gap between the legal statutes and the actual situation in the electronic world. Investigating and prosecuting cyber-stalking presents

50 www.canlii.org

51 http://rangi.knowledge-basket.co.nz.

unique challenges. Establishing a pattern of harassment is critical to an investigation as well as to identifying the stalker's true identity, which may be unknown to the victim due to the anonymous nature of the Internet. Victims must maintain copies of all online correspondence from the stalker, such as e-mails, chat room conversations, and websites, as evidence which law enforcement agencies can investigate. Victims should notify law enforcement agencies when online communications become threatening or cyber-stalkers approach their targets in the real world[52].

When identifying cyber-stalking in the field, particularly when considering whether to report it to any kind of legal authority, the following features or combinations of features can be considered to characterize a true stalking situation:

The manifest desire and intention to terrorize and hurt somebody. Much cyber-stalking is malicious in nature due to the presence and communication of clear and direct threats. Not all cyber-stalking however is malicious[53]. In cases of love-oriented obsessive cyber-stalking for example, the stalker has no visible intent to harm, and while their behavior may cause great distress, they do not necessarily realize that this is happenning. Other forms of online harassment are also not necessarily malicious. Some online harassment takes the forms of practical jokes, and while this may be unpleasant and cause great inconvenience, annoyance, fear or distress, the harasser may not have intended to cause harm.

Not all harassment is premeditated either. Sometimes it may be the result of a sudden emotional outburst, where someone loses his temper and lashes out electronically. This may indeed cause distress but could not be called premeditated, since the attack was sudden and not planned.

Repetition is a key feature of online stalking. A one-off attack online, while it may cause distress, could not be described as cyber-stalking. Cyber-stalking is a course of conduct that takes place over a period of time and involves repeated attempts to causing distress. Some laws even define it as involving two or more incidents and following a repetitive pattern.

One could not claim cyber-stalking or even online harassment if distress is not felt in some way. Distress can take many forms, from annoyance, offense, inconvenience and humiliation, to worry and fear for safety. The presence of fear is an important characteristic of cyber-stalking.

One also needs to be careful that is not over-reacting. In legal terms, stalking is usually defined as a course of conduct that causes a reasonable person to be in distress.

Proving distress as a result of online stalking might be difficult. It needs the testimony of expert witnesses, or proof that the victim went to a doctor for help or medication concerning the incident.

52 www.nw3c.org

53 www.wiredsafety.org/cyberstalking_ harassment/definition.html

The anonymity of electronic communications could also pose a difficulty. Though a victim may know the identity of his or her aggressor, the prosecutors have few chances to prove a connection between the sender and the accused. It is important that more expertise is acquired about (local and virtual) stalking, and that special units are established to deal effectively with these offences. Most police and juridical institutions still have insufficient experience to recognize the serious nature of cyber-stalking and to investigate these crimes.

The disparity[54] in the activity level among law enforcement agencies can be attributed to a number of factors. First, it appears that the majority of cyber-stalking victims do not report the conduct to law enforcement, either because they feel that the conduct has not reached the point of being a criminal offense, or that law enforcement will not take them seriously. Second, most law enforcement agencies have not had the training to recognize the serious nature of cyber-stalking and to investigate such offenses. Unfortunately, some victims have reported that rather than open an investigation, a law enforcement agency has advised them to come back if the cyber-stalkers confront or threaten them off-line. In several instances, victims have been told by law enforcement simply to turn off their computers.

The Suggested Solution

Jurisdictions around the world are now only starting to recognize cyber-stalking as a criminal offense. The fear of victims of cyber-stalking is just as real as with any other crime. It is therefore important to develop a comprehensive and effective plan for dealing with cyber-stalking. Only when this is done will the Internet be a safer place for web users. Until the law on cyber-stalking has been fully developed, victims should educate themselves on the methods of effectively handling on-line harassment.

Self-protection, while essential, is not sufficient to make cyber-space a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber-crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current statutes to determine whether these are sufficient to combat the cyber-crimes.

Effective law enforcement is complicated by the transnational nature of cyber-space[55]. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber-criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign

54 www.mcconnellinternational.com
55 http://www.Internetcrimes.com

sources[56]. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber-crimes like cyber-stalking.

A future international law statute should criminalize the use of images, signs, language for the willful purpose of systematically threatening, harassing, intimidating, tormenting or embarrassing, directly or indirectly, another person through electronic devices, e-mail or over the Internet. Upon conviction, cyber-stalking should then be punished with fines and imprisonment.

56 http://www.haltabuse.org

CHAPTER 10. IDENTITY THEFT

The Problem

Identity Theft is a truly modern crime, being crafted out of the sight of, and often beyond the effective reach of, the victim. It is carried out by compromising electronic data systems, obtaining false primary documents, directing mail to new addresses, obtaining new credit accounts and improperly charging existing ones. It can be accomplished by a neighbor next door or by criminals hunting from thousands of miles away. It relies on the facility of modern technology and superficial consumer security.

Identity theft is the unauthorized collection and fraudulent use of key pieces of information, such as social security or driver's license numbers, in order to impersonate someone else[57]. The information can be used to obtain credit, merchandise, and services in the name of the victim, or to provide the thief with false credentials. In addition to running up debt, an imposter might provide false identification to police, thus creating a criminal record or leaving outstanding arrest warrants for the person whose identity has been stolen. Victims of identity theft suffer financial loss, damage to their reputation, and emotional distress, and are left with the complicated and sometimes arduous task of clearing their names.[58]

Identity theft is categorized in two ways: True Name and Account Takeover.

- True Name Identity Theft means that the thief uses personal information to open new accounts. The thief might open a new credit card account, establish cellular phone service, or open a new checking account in order to obtain blank checks.
- Account Takeover Identity Theft means the imposter uses personal information to gain access to an existing account. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes that there is a problem.

A new form of identity theft is *phishing*[59], which occurs when scammers send mass e-mails posing as banks, credit card companies, or popular commercial web-sites, asking recipients to confirm or update personal and financial information in a hyperlink to a look-alike web-site for the spoofed company, and usually threaten suspension or deactivation of accounts for non-compliance. Many of the emails claim to be anti-fraud departments at the institutions alerting the recipients to nonexistent suspicious transactions.

57 www.privacyrights.org/fs/fs17-it.htm

58 Lawson Philippa and Lawford John, Identity Theft: The Need for better consumer protection, Canadian Cataloguing and Publication Data, Ottawa, Canada, Nov 2003.

59 www.aba.com/Industry+Issues/eAlertNews05.htm

The Internet has made it easier for identity thieves to use the information they have stolen because transactions can be made without any personal interaction. Computers make it possible to reduce the risk of personal harm to the criminal by decreasing the probability of detection, and therefore punishment, while at the same time significantly increasing the expected return.

The Existing Texts

Combating identity theft is difficult because each state or group of states has a different idea about how to combat the issue, about how much privacy invasion is allowed under a crime-fighting or civil litigation plan, and about what system would be useful for regulating and granting jurisdiction[60].

As a consequence, laws regulating identity theft differ in content in different countries. On the one hand, European States do not expressly criminalize the identity theft, while on the other hand, United States legislation sets up the toughest penalties. In 1998, the US Congress passed the Identity Theft and Assumption Deterrence Act, making identity theft a crime punishable by up to 15 years of imprisonment. In July 2004, the Identity Theft Penalty Enhancement Act stiffened penalties for the crime of identity theft even further, and established a new federal crime of aggravated identity theft for such serious offenses as bank fraud or defrauding employee benefit plans. Under the new law, those convicted of aggravated identity theft must serve an additional mandatory two-year prison term and enhanced five-year consecutive penalties if a terrorist-related offense occurs.

USA

Federal Trade Commission-Assumption Deterrence Act, June 1998

a. The term document-making implement means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement;

b. The term identification document means a document made or issued by or under the authority of the United States Government, a State, political subdivision of a State, a foreign government, political subdivision of a foreign government, an international governmental or an international quasi-governmental organization which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals;

c. The term 'false identification document' means a document of a type intended or commonly accepted for the purposes of identification of individuals that is not issued by or under the authority of a governmental entity; and appears to be issued by or under the authority of the United States Government, a State, a political subdivision of a State, a foreign government, a political subdivision of a foreign government, or an international governmental or quasi-governmental organization;

60 Erin Suzanne Davis, A World Wide Problem on the World Wide Web:International Responses to Transnational IdentityTheft via the Internet.

d. The term means of identification means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any

-name, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

-unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

- unique electronic identification number, address, or routing code;

-telecommunication identifying information or access device.

e. The term personal identification card means an identification document issued by a State or local government solely for the purpose of identification;

f. The term produce includes alter, authenticate, or assemble;

g. The term transfer includes selecting an identification document, false identification document, or document-making implement and placing or directing the placement of such identification document, false identification document, or document-making implement on an online location where it is available to others.

EUROPEAN UNION

Council Directive 95/46 EC 1995-Data Protection

a. personal data shall mean any information related to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity ;

b. processing of personal data (processing) shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure, by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Council of Europe Committee of Experts on Crime in Cyber-Space, Convention on Cyber-crime 2001

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another by :

a. any input, alteration, deletion or suppression of computer data ;

b. any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another.

JAPAN

Japanese Privacy Act -2003

The Basic Principles of the Japanese draft law require:

a. use of personal information for a clearly defined purpose and within the scope necessary for the achievement of that purpose;

b. the use of lawful and proper means to acquire personal information;

c. maintenance of the accuracy and currency of personal data;

d. the implementation of appropriate measures to maintain the security of personal information;

e. allowing individuals access to their personal information.

The Basic Principles were to be applied without exception to the personal information-handling practices of all individuals and of all public and private sector organizations.

The Loopholes

In addition to criminalizing certain types of activities, the European Convention attempts to foster cooperation between countries in prosecuting computer crimes[61]. It promotes uniform national legislation, common criminal procedures, and resources for cooperation on an international level. In this sense the Convention holds perpetrators of computer crimes responsible for these acts even if their own countries do not consider the acts to be criminal, but does not however provide means for cross-border investigations of cyber-crimes.

The Convention lacks data protection laws necessary to curb identity theft and its effects because it does not provide victims of identity theft with civil remedies. It also does not adequately address the types of personal information identity thieves use to perpetrate their crimes, such as social security numbers.

The European Union also passed a Directive in 1998 designed to restrict data collection, processing, dissemination, and storage in Europe. The directive encompasses all types of personal data, but is not self-executing; it requires states to create implementing legislation on their own. The Directive also requires that member states enact laws prohibiting the transfer of data to non-member states that fail to ensure an adequate level of protection. Due to differing traditions and approaches to privacy protection, different states also view this adequacy requirement in divergent manners. As the system is based on individual national laws, the Directive lacks the enforcement power that it seeks.

Complications arise from the fact that member states can opt out of the exceptions allowed under the Directive. The adequacy requirement complicates uniformity for many of the same reasons as self-execution of the regulatory laws. By allowing individual states to enforce the adequacy requirement against non-member states, non-member states run the risk of having EU states destroy their information, deny them access to the EU market, or instigate legal proceedings against them.

The European approach to combating cyber-crime advocates stricter controls to protect consumers as compared to e-commerce companies. Europeans consider personal privacy to have greater importance and commercial concerns are addressed as secondary to this concern.

61 http://law.wustl.edu/Journal/12/p201%20Davis.pdf

In the US, the Federal Trade Commission has not provided adequate protection for consumers and as a result, the basic principle is one of industry self regulation. The United States is concerned that data protection laws are too strict and will have a potentially regressive impact on international commerce. The EU Convention, based as it is on European ideals, does not offer the kind of free access to personal information to which US businesses are accustomed. This US system opposes[62] the traditional European practice of recognizing privacy as a basic individual right.

Although identity theft is on the cutting edge of technology, what is criminal in one country is not criminal in many other countries, and therefore many international investigations end without the prosecution and punishment of responsible criminals. A standardization of the legal regimes of so many countries will undoubtedly enhance international cooperation in on-line identity theft investigations and prosecutions. The current structure of international mutual legal assistance is much too slow and cumbersome for the Internet Age. Electronic evidence is ephemeral, and the delay inherent in the current structure significantly lessens the chance that such evidence will be obtained and that identity thieves will be caught and prosecuted.

The Suggested Solution

The international community needs to focus on active and collaborative enforcement because the Internet is an environment in which it is much easier to perpetrate an identity theft than in the real world.

In order for a treaty dealing with identity theft to be successful, other non-European and non-American countries must also be encouraged to participate. The Council of Europe Convention on Cyber-crime is a step in this direction but must be expanded to include other parts of the globe, as well as crime specific laws and civil remedies dealing with data protection and identity theft.

The ideal treaty on identity theft must also create laws that do not depend only on industry self-regulation. Its provisions must force credit companies to adhere to policies that prevent identity theft crimes and, at the same time, allow victims to gain the information and protection they need to restore their credit records and prevent future breaches of their accounts.

Another step that an international coordinated effort may need is to try to control identity theft crimes on an international level. In order to succeed globally, states may have to reexamine the concept of sovereignty and to surrender some so that global cooperation against cyber-crime is realized.

62 law.wustl.edu/Journal/12/p201%20Davis.pdf

CHAPTER 11. CYBER-TERRORISM

The Problem

With the increased exposure to and dependence on Internet connectivity and dependent services, government, media and the public have also increasingly given more attention to the potential threat of cyber-terrorism to these Internet-connected systems, particularly for the critical information infrastructures of nation states.

While a definition of terrorism has eluded the international community for decades, it is generally agreed that a terrorist act implies the use of violence for political objectives and for the purpose of sowing fear within a target population.

Cyber-terrorism[63] is but one form of cyber-attack. Too often the terms cyber-terrorism and cyber-attack are used interchangeably and may result in a misunderstanding of the cyber-threat in general, and the threat of cyber-terrorism in particular. Politically motivated cyber-attacks that lead to death or bodily injury, explosions, or severe economic loss would be dear examples of cyber-terrorism.

Terrorism in cyber-space is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. To qualify as cyber-terrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyber-terrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not.

Cyber-terrorism[64] is indeed a grave crime considering the substantial losses that even a single successful operation can generate. Cyber-space is constantly under assault from cyber-spies, thieves, saboteurs, and thrill seekers break into computer systems, steal personal data and trade secrets, vandalize Web sites, disrupt service, sabotage data and systems, launch computer viruses and worms, conduct fraudulent transactions, and harass individuals and companies. These attacks are facilitated with increasingly powerful and easy-to-use software tools, which are readily available for free from thousands of web- sites on the Internet. Therefore we should also categorize as cyber-terrorism those attacks that cause less than total or partial destruction, like slowing down the performance of a machine or a server system, and thus produce financial consequences.

63 http://www.cs.georgetown.edu/~denning

64 Putting cyber-terrorism into context, 24 October 2003by Kathryn Kerr

In contrast, cyber-terrorism has been used improperly to refer to the use of:

- encryption technologies for secure electronic storage of data and communication by and between supporters/members of known terrorist groups;
- various forms of electronic communications (web sites, email etc) for the purposes of recruiting supporters, organizing and communicating the messages (propaganda) of known terrorist groups;
- the occasional use by known terrorist groups of cyber-attack techniques which are incapable of causing bodily harm, fear or serious economic damage; and
- the occurrence of port scans from countries considered to sponsor terrorism or which harbor known terrorist groups.

There is a major difference between cyber-crime and cyber-terrorism. Cyber-terrorism aims to wreak casualties and destruction through cyber-space, allowing attackers to remain far from the target. In contrast, cyber-criminals seek profits, and could focus on illegal transfer of funds, money laundering, Internet fraud, tax evasion, and communications between criminal organizations.

It is therefore prudent to distinguish between cyber-crime (an unlawful act wherein the computer is either a tool or a target or both), and cyber- terrorism. Cyber-terrorism is the premeditated use of disruptive activities, or the threat thereof, in cyber-space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in the furtherance of such objectives.

There are a number of reasons why cyber-terrorism is a very attractive[65] option for terrorists. Firstly, it is cheaper than traditional terrorism methods. All that the terrorist needs is a personal computer and a simple telephone connection. Terrorists do not need to buy traditional offensive weapons such as guns and bombs; instead they can create and deliver computer viruses through a telephone line. Also, terrorists do not need to rent vehicles or to pay someone to deliver their explosives; they can deliver their terror from their home computer.

Secondly, cyber-terrorismis is more anonymous[66] than traditional terrorist methods. It is simply difficult to track a cyber-terrorist. There are no physical barriers such as checkpoints, customs agents, or borders which are crossed. Criminals in the physical world have long employed the tactics of masking their true identity with disguises and aliases. It should come as no surprise then, that criminals who conduct their nefarious activities on networks and computers should employ similar techniques. *"IP spoofing"* is one of the most common

65 http://www.washingtonmonthly.com/features/2001/0211.green.html
66 Is Everyone an Enemy in Cyber-Space? Ariel T. Sobelman

forms of on-line camouflage. In IP spoofing, an attacker gains unauthorized access to a computer or a network by making it appear that a malicious message has come from a trusted machine by "spoofing" the IP address of that machine. It should not be difficult to detect this maneuver because there are very feasible technologies available to counter this spoofing now.

Thirdly, there are an exponentially large number of targets. These could be government computers, corporation computers, individual computers, public works, private airline computers, etc. Within each of these categories of computers there are sub-categories of systems and networks that can be hacked into. Another appealing factor is that the law of averages dictates that with this many computers and networks, there will be a large number of weaknesses and vulnerabilities that the terrorists can exploit.

Fourthly, cyber-terrorism can be conducted remotely. This feature of cyber-terrorism is especially appealing to cyber-terrorists. Typically, terrorists using traditional methods, such as suicide bombing, spend a great deal of time and money recruiting and training terrorists who eventually die carrying out their attacks. Cyber-terrorism would result in terrorist groups retaining a larger number of followers in relative safety.

Finally, cyber-terrorism has the potential to affect a larger number of people than traditional terrorist methods[67]. For example, it was estimated that the *I Love You* virus affected more than twenty million Internet users and cost billions of dollars in damage. Because cyber-terrorism can affect more people, there is the potential for a greater degree of media coverage, which is ultimately what a terrorist wants.

It seems that the presence of firewalls and advanced encryption technology has not prevented intrusions, the theft of trade secrets, and the wreaking of havoc in government bodies. Many experts continue to warn of the persistence of a number of terrorist organizations attempting to develop new generations of viruses to launch wide-scale cyber-attacks.

Fears of cyber-terrorism attacks[68] cover a number of scenarios including, developing a virus that enables the control of telephones throughout a community and prompts them to all simultaneously dial the emergency number in order to to paralyze the emergency service. Losses would be heavier should this paralysis be accompanied by a bomb explosion in a market or building.

The rise of terrorism, as one type of asymmetric and distributed warfare, has not only threatened the gains derived from cyber-space, but has threatened the activities that now come to depend on communication through cyber-space infrastructure. Individuals and governments wish to ensure that they will continue to reap the benefits of cyber-space, and that cyber-space controls will not be turned against them. Their enemies see cyber-space as a high-value

67 cyber-crimes.net/Terrorism/ct.html - 57k

68 Cyber-terrorism And Computer Crimes: Issues Surrounding The Establishment Of An International Legal Regime by Richard W. Aldrich

target. It is legimately feared that terrorists may have developed an academy of cyber-terrorism, seeking means to attack the cyber-space infrastructure of the West.

Public opinion [69] and dramatic attacks on computer networks could provide a means to do this with only small teams and minimal funds. Moreover, virtual attacks over the Internet or other networks allow attackers to be far away, making borders, X-ray machines, and other physical barriers irrelevant. Cyber-terrorists would not need a complicit or weak government to host them as they train and plot. On-line attackers could also cloak their true identities and locations, choosing to remain anonymous or pretending to be someone else.

Terrorists might also try to use cyber-attacks to amplify the effect of other attacks. For example, they might try to block emergency communications or cut off electricity or water in the wake of a conventional bombing or a biological, chemical, or radiation attack. Many experts believe that this kind of coordinated attack might be the most effective use of cyber-terrorism.

Cyber-terrorism could also involve the destruction of the actual machinery of the information infrastructure; remotely disrupting government computer networks, or critical civilian systems such as financial networks; or using computer networks to take over machines that control traffic lights, power plants, or dams in order to wreak havoc.

Attacks could also involve remotely hijacking control systems, with potentially dire consequences: breaching dams, colliding airplanes, shutting down the power grid, etc.

The Existing Texts

USA

Section 814 of The Patriot Act158 is titled Deterrence And Prevention Of Cyber-terrorism. This section amends section 1030(a) (5) of title 18, United States Code. The amended section punishes any person who causes unauthorized damage to a protected computer159 by either:

(i) knowingly causing the transmission of a program, information, code, or command, or
(ii) intentionally and unauthorizedly accessing a protected computer

This section applies only in cases where the conduct of the accused causes:

(i) loss to one or more persons during any 1-year period aggregating at least $5,000 in value, or
(ii) the actual or potential modification or impairment of the medical examination, diagnosis, treatment, or care of one or more individuals, or
(iii) physical injury to any person, or
(iv) a threat to public health or safety, or

69 In Fear Of Cyber-terrorism: An Analysis Of The Congressional Response Tara Mythri Raghavan

(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security.

Section 816 of The Patriot Act is titled Development and Support of Cyber security Forensic Capabilities. This section *empowers the Attorney General to establish adequate regional computer forensic laboratories and provide support to existing computer forensic laboratories, in order that all such computer forensic laboratories have the capability to:*

1) provide forensic examinations with respect to seized or intercepted computer evidence relating to criminal activity (including cyber-terrorism),

2) provide training and education for Federal, State, and local law enforcement personnel and prosecutors regarding investigations, forensic analyses, and prosecutions of computer related crime (including cyber-terrorism),

3) assist Federal, State, and local law enforcement in enforcing Federal, State, and local criminal laws relating to computer-related crime,

4) facilitate and promote the sharing of Federal law enforcement expertise and information about the investigation, analysis, and prosecution of computer related crime with State and local law enforcement personnel and prosecutors, including the use of multi jurisdictional task forces, and

5) carry out such other activities as the Attorney General considers appropriate.

UNITED KINGDOM

As per The Terrorism Act, 2000165, the term terrorism includes the use or threat of action that is

i) designed seriously to interfere with or seriously to disrupt an electronic system

ii) designed to influence the government or to intimidate the public or a section of the public, and

iii) made for the purpose of advancing a political, religious or ideological cause.

INDIA

Although the term cyber-terrorism is absent from the terminology of the Indian law, section 69 of the Information Technology Act is a strong legislative measure to counter the use of encryption by terrorists.

This section authorizes the Controller of Certifying Authorities (CCA) to direct any Government agency to intercept any information transmitted through any computer resource. Any person who fails to assist the Government agency in decrypting the information sought to be intercepted is liable for imprisonment up to 7 years.

EUROPE

Cyber-crime and Cyber-terrorism: the Council of Europe Cyber-crime

The 2001 Council of Europe Cyber-crime Convention addresses cyber-crime broadly, and deals with a number of legal issues, including harmonization of substantive law, harmonization of certain procedural aspects of investigations, and facilitation of mutual legal assistance.

Under this Convention, states are required to establish a number of defined offenses, including crimes against the confidentiality, integrity and

availability of computer systems, their processing capacity and their data content (articles 2-6). These provisions require states to prohibit most types of cyber-terrorism.

Under the Convention, each member state is required to establish laws that will enable it to intercept, preserve, search and seize data on its networks. These include real-time monitoring of traffic data (article 20) and interception of content data (article 21).

Article 22 of the Convention provides that each party shall extend its jurisdiction over offences committed in its territory or by its nationals.

Perhaps the most important and interesting parts of the Convention are the provisions dealing with international cooperation, including extradition and mutual assistance (articles 23-35). A broad range of cyber-crimes are made extraditable offenses, and signatories are required to provide mutual assistance to the widest extent possible in connection with the preservation and collection of requested data. Much of the Convention is oriented toward law enforcement after the commission of a crime, rather than the interdiction of the crime or cyber-terrorism. Article 31 deals with mutual assistance regarding access to stored computer data; article 33 deals with mutual assistance with respect to real-time collection of traffic data and article 34 deals with mutual assistance with respect to interception of content data. Thus, it can be said that the Cyber-crime Convention is a cyber-crime law enforcement convention, not a cyber-terrorism convention. While it would be expected to have some incremental benefits against cyber-terrorism, it could not be expected to substantially reduce the risk of cyber-terrorism by the more dedicated actors.

The Loopholes

Connections via the Internet and other networks continue to develop, and interdependence increases[70]. There is also increasing an standardization and commonality in the specifications of information systems. These trends increase the threat of cyber-attacks, even on information systems that currently face little danger from outside intrusion. In addition, there is always the possibility of such attacks being made by disgruntled inside personnel. Even an information system that is not connected to any other networks is not immune to the danger of an outside attack[71].

The present attempts to define and understand cyber-terrorism remain mired in biases that continue to perpetuate the myths surrounding conventional terrorism. Knowledge of the *who* and *what*[72] of cyber-terrorism is limited to ambiguous interpretations of terrorist actors and speculative extrapolations of potential terrorist activity. In both of the cases, cyber-terrorism has become a catch-all term that can be pulled from the bag to fit any

70 www.bits.go.jp/en/sisaku/cyber_terror.html

71 www.kantei.go.jp/foreign/ it/security/2001/cyber_terror.html

72 www.comm.ucsb.edu/Research/ Myths%20and%20Realities%20of%20Cyberterrorism.pdf

number of scenarios or purposes. For the policymaker, this means that political expediencies often dictate what should be pragmatic measures. It is also essential to remember that for the victim, the type perpetrator behind the attack is often less important than the consequences of the attack.

To the innocent bystander caught in the crossfire or explosion connected to a terrorist incident there is no doubt that the incident and his/her victimization is random and hence even more terrifying. However, the reality of terrorism is that it is purposeful and involves selectivity in its execution. These reveal a distinctive set of patterns which suggest that factors such as environment and terrorist group composition play significant roles in the nature of the terrorism that transpires. More specifically, terrorist groups develop their *modus operandi* based on where they originate, who supports them, who their enemies are, what their likelihood of success will be and a host of other tactical and strategic considerations. For example, nationalist/ethnic based terrorist groups clearly have developed primary spheres of operation and in general focus their attention on specific targets related to their goals. Such terrorist groups engage in terrorist activity for a predetermined political purpose and their goals are not furthered by random attacks which the public (their audience) cannot interpret. Although the last three decades have witnessed thousands of international terrorist incidents they have more often than not been of a deliberate rather than random nature.

The assumption that terrorism knows and respects no boundaries flows from the same base that perpetuates the assertion that terrorism is random and indiscriminate. While it is correct to suggest that the entire international system has experienced international terrorism at one time or another, it is more accurate to argue that a relatively small group of states are the constant targets of international terrorism, while the vast majority reside on the periphery of this violence. Empirical evidence that over half of all international terrorism has been perpetrated in just thirteen states and less than seven states account for over fifty per cent of all victimization, indicates the reality of terrorism. Further evidence also suggests that the majority of terrorist acts are not characterized by the large-scale needless killing and destruction that is so often assumed.

Because terrorism can conceivably cover a full spectrum of violence from non-lethal threats, to simple destruction of property, to mass loss of life, there is considerable room for interpretation about its nature[73]. Instead of relying on this conceptualization as the sole standard for judging terrorist violence, it is more helpful to place individual terrorist acts in the context of larger terrorist campaigns. In order to achieve their goals, regardless of how irrational the goals might appear to outsiders, terrorist groups must engage in some level of rational behavior. To do otherwise would compromise the very existence of

73 www.comm.ucsb.edu/Research/ Myths%20and%20Realities%20of%20Cyberterrorism.pdf

the group. Groups that focus all their efforts on wild forays into violence characterized by mass killing are not likely to survive. Terrorist groups need the support of wider constituencies in order to survive. This support is generally not forthcoming if terrorist incidents are deemed too violent or beyond the accepted limits of the constituency. While many constituencies will support violence against government officials, soldiers and others seen as representing the occupiers or repressors, it is difficult for most groups to sustain the support of their constituencies for acts of terror against innocent civilian populations, particularly if there are widespread civilian victims.

Terrorist groups must also deal with a heightened state response to particularly violent acts[74]. Bombs placed outside of protective embassy walls do not elicit the same pressure for counter-terrorist response as bombs placed on airliners. Finally, terrorist groups must reconcile their use of violence with their own ideologies. If terrorist groups are to survive and thrive careful attention must be paid to the exact nature and objective of their terrorist campaigns.

Despite its vicious notoriety, the data [75] indicates that international terrorism results in less than one fatality per incident and over ninety per cent of the incidents have not resulted in the death of any victims. There are also relatively few high-end incidents such as the bombing of airliners. In fact, there were only twenty-one bombings of airliners over a twenty-seven year period and only twelve resulted in the deaths of more than twenty people[76]. The foundation of terrorism to date has been a combination of threatened violence with an assortment of other violent acts that have produced proportionally more fear than death or destruction.

Although states have traditionally been considered as society's neutral conflict manager, a more accurate view treats them as interested parties. In this conceptualization the role of states as keepers of order is expanded to include instances where non-state actors have acted with a state's political interests in mind. In other words, there are circumstances where the terrorist activity of non-state actors is accepted as order inducing rather than chaos inducing.

State support for non-governmental terrorism also extends to the international arena. Again, there are instances where the terrorism of non-state entities coincides with the national interests of sovereign states. State support in this respect generally depends on a cost-benefit analysis that calculates the benefit thought possible from the desired outcome, the believed probability with which the action will bring about, the desired state of affairs, and the believed probable cost of engaging in the action. International non-state terrorism supported by states is an example of surrogate terror. More specifically, this terrorism appears as:

74 www.globalsecurity.org/ military/library/report/1984/CR.htm

75 www.comm.ucsb.edu/Research/ Myths%20and%20Realities%20of%20Cyberterrorism.pdf

76 www.comm.ucsb.edu

- State-supported terrorism: An occurrence where the initial terrorist actions of third parties are subsequently supported by interested states; or
- State acquiescence: Instances where the terrorist activity of non-state actors is tacitly approved or at least not condemned;

In both of the above cases, the actions of states are at odds with the myth that these actors always oppose state terrorism. This reality is also in direct contrast with another widely held belief, that terrorism is a weapon of the weak. Even the most powerful states have found that support for non-state terrorism serves a purpose in international relations.

With the advent of terrorism involving computer networks it is unrealistic to believe that only non-state actors will use the cyber-environment as a new arena of terrorism.

The analysis of terrorism in the cyber-environment must critically assess all origins and sources of terrorism. If the myth of satanic actors persists into the next generation of terrorism, many opportunities for countering the phenomenon will be lost. All of the assertions outlined above inhibit clear thinking on the subject of terrorism and are equally important in terms of understanding the terrorism that is both conventional and cyber in nature.

The Suggested Solution

Anti-cyber-crime security specialists acknowledge that the attacks that have been launched to date have been relatively unsophisticated. The possibility of broader and better organized attacks, however, prompts great concern.

The international community should take more interest in furthering agreements that introduce the necessary legislation to combat these crimes. This should include, among othere aspects, a discussion on establishing an early warning system for cyber-attacks, developing more secure software, and making executives and consumers more aware of the need for safer Internet usage.

The capacity of organizations and governments to repel cyber-threats needs to be enhanced. The technology required to confront such threats must be developed by increasing computer-network security through advanced encryption systems and firewalls in networks, by more accurate hacker-detection systems, and by stronger anti-virus programs.

The threat of cyber-attack for organizations with Internet connections is high. For the most part this threat has little to do with the occurrence of conventional terrorist attacks, increased international tensions or nation state conflicts. Certainly, these events may increase the threat of politically motivated web site defacements or other forms of politically motivated low impact cyber-attack, but only slightly.

There is still much to be done, and as the field of cyber-technology[77] takes on new and better dimensions, the tools that are needed to address the growing threats to this field must also be enhanced, redefined, and reorganized. There is a dictum among computer hackers that *"no system, however impenetrable it can be, will stand against a determined hostile attack, if that system itself does not equally understand the minds of the people that carry out these attacks"*[78]. The threat[79] now is one that traditionalists cannot readily fathom, because the cyber-space that they operate on affords them anonymity. With faceless enemies, our analytical hands are clipped and we are left wondering about what had hit us.

We must address the issues of, first, the institutionalization of a mechanism to prevent and suppress cyber-crime and cyber-terrorism at the onset, and second, the convergence of a legal framework that will address both national and transnational issues on enforcement, cooperation, prevention, and investigation of transnational crimes, including computer crimes. This requires among others:

- Appropriate laws and regulations on information security fundamentals and trained personnel to ensure its widespread application, which must lead ultimately to further development of countermeasures to cyber-terrorism.
- A wider understanding by the operators and users of general information systems of the threat of cyber-attacks, and of the necessary security countermeasures so that there is a widespread general awareness and effort to handle this issue.
- Since cyber-attacks can be generated without regard for national boundaries, so international cooperation and coordination is essential in order to handle such attacks.
- As a key infrastructure operator, the private sector must work with governments to accumulate information on information security problems.
- Governments, in turn, must promote cooperation with international organizations in the field of cyber-terrorism.

In the first place, there is an immediate need to to criminalize all the attacks and threats through or against computer networks which intimidate or force a government or a people through violence or similar harm. Depending on the social danger that is posed, cyber-terrorist crimes must be punished with long terms of imprisonment to better advance prevention. For this to be effective, states must implement harmonized legal regulations on a domestic level, and use the instrument of legal extradition whenevr necessary.

77 Global Cyber-terrorism, Jurisdiction, and International Organization Joel P. Trachtman
78 www.pctc.gov.ph/edocs/updates/cybercrm.htm
79 Myths and Realities of Cyber terrorism Peter Flemming and Michael Stohl

CHAPTER 12. CYBER-WAR

The Problem

Cyber-War, or information warfare waged over the Internet, basically involves the infiltration and disruption of an enemy's computer networks and databases, often with the use of weapons such as viruses, worms, trojan horses and the new electro-magnetic pulse wave[80] weapon. The latter is particularly worrisome as the capability now exists to generate an instantaneous electromagnetic pulse that will overload and destroy the sensitive circuitry in advanced electronics and computer systems without any detonation of weapons in the upper atmosphere. Any system that is within the limited range of these weapons will be disrupted or have its electronic components destroyed. An electromagnetic weapon does not leave a crater like a conventional bomb, nor does it modify the operating system of a computer, and as a result the detection of an attack becomes more difficult.

Military doctrine, organization and strategy have continually undergone profound, technology-driven changes throughout history. Industrialization led to attrition warfare by massive armies in World War I. Mechanization led to maneuver predominated by tanks in World War II. The information revolution implies the rise of a new mode of warfare in which neither mass nor mobility will decide outcomes; instead, the side that has greater technological knowledge will enjoy decisive advantages. The information revolution sets in motion forces that challenge the design of many traditional institutions. It diffuses and redistributes power, often to the benefit of smaller actors. It crosses borders, redraws boundaries, and generally compels closed systems to open up. The information revolution caused shifts, both in how societies may come into conflict, and how their armed forces may wage war.

In previous wars, critical infrastructure components such as airports, power plants, water systems, railroads, oil and gas pipelines, and communication centers were targeted by the military because their destruction could help cripple a nation. These same components no longer have to be physically destroyed because most are dependent on computer-based systems that could be more easily disabled in a cyber-attack.

Cyber-war[81] comes under what military theorists increasingly refer to as asymmetric warfare, whereby unconventional tactics are used by smaller players to offset their military weaknesses. Like a classic guerrilla struggle, which is a conflict of the weak against the strong, cyber-war can enable an individual to damage the computer system of a government or down the website of a multinational corporation. The weapon of choice can be nothing more than a laptop computer wired to the Internet.

80 http://www.fas.org/irp/threat/cyber/docs/npgs/ch2.htm
81 http://www.rand.org/publications/randreview/issues/RRR.fall95.cyber/Cyber-war.html

In cyber-war, one single individual can target the chink in the armor of modern technology[82]: that no computer system is totally invulnerable to attack from a talented and determined hacker. It is a form of warfare that can be conducted remotely and anonymously. Cyber-war may be less bloody but it is potentially highly destructive with far-reaching effects. Other possible scenarios include cyber-attacks on the websites and databases of businesses, on the Internet route-server infrastructure itself, as well as on public utility networks involving, for example, the tampering with electrical grids, the shutting down of telephone systems, the paralyzing of banking systems, and of rendering air traffic control systems inoperable. Whether the hackers on either side are labeled as terrorists or freedom fighters, or whether cyber-war is practiced as deliberate state policy, online warfare looks set to become a key part of today's era of connectivity and globalization.

Cyber-war can thus take various forms. It may occur between the governments of rival nation-states. It may arise between governments and non-state actors, but financed nevertheless by states. It may be waged against the policies of specific governments by advocacy groups, involving, for example, environmental, human rights, cultural, or religious issues. Non-state actors may or may not be associated with nations, and in some cases they may be organized into vast transnational decentralised coalitions.

In the case of cyber-risks[83], almost everything is new. The weapons are not kinetic, but software and knowledge; the environment in which he attacks occur is not only physical, but virtual; the possible attacker, even if it is a government, is able to hide effectively even during an attack. This form of warfare may involve diverse technologies, notably for command and control, for intelligence collection, processing and distribution, for tactical communications, positioning, identifying friend-or-foe, and for smart weapons systems. It may also involve electronically blinding, jamming, deceiving, overloading and intruding into an adversary's information and communications circuits.

Decisive changes[84] are occurring in how information is collected, stored, processed, communicated and presented, and in how organizations and governments are designing themselves to take advantage of this change. Information is now a strategic resource.

Cyber-war thus has broad ramifications for military[85] organizations. Cyber-war now implies the development of new doctrines about the kinds of forces needed, where and how they are to be deployed, and how to strike the enemy. How and where to position what kinds of computers, sensors, networks and

82 Resolving the Legal Issues Concerning the use of Information Warfare in the International Forum: The Reach of the Existing Legal Framework, and the Creation of a New Paradigm by Michael J. Robbat

83 The Future of Information Security by Martin Libicki

84 Cyber-war Is Coming by John Arquilla and David Ronfeldt

85 http://www.soci.niu.edu/~crypt/other/wsj.htm

databases may become as important as the question once was for the deployment of bombers and their support functions.

As an innovation in warfare, cyber-war may be to the 21st century what blitzkrieg was to the 20th century. At a minimum, cyber-war represents an extension of the traditional importance of obtaining information in war: having superior command, control, communication and intelligence and trying to locate, read, surprise and deceive the enemy before he does the same to you.

The premise behind cyber-war is how to subjugate the enemy without fighting. It is designed to disable an enemy's armed forces and civilian infrastructure without the use of a single bullet. The computer will be the weapon of the 21st century.

The attractiveness[86] of wartime use of information rests on the application of the theory that it may be more efficient to attack an enemy infrastructure than to confront military forces on the battlefield. The strategy of attacking the civilian sector of a nation as a way to defeat its armed forces in the field is not a new one. In the late nineteenth century, military forces began to rely on industry for sustenance. This dependence has progressed to the point where wars are no longer aimed at defeating the enemy on the battlefield; they are wars of attrition, in which victory can be attained only through the destruction of the state itself, and the morale of its civilian population.

Current military theory[87] suggests therefore that attacking a nation's centers of gravity, in addition to its armed forces, is the most effective way to destroy the state. In today's societies centers of gravity include telecommunications networks, energy and power sources, transportation systems, and financial centers and networks. Thus, the destruction of these systems becomes just as important as destroying an adversary's military forces.

Not only will cyber-war be a force in future warfare, it may also turn out to be the great equalizer for nations attacking adversaries with superior conventional military power. Most nations lack the resources to build a military machine and may use information technologies to overcome their battlefield inferiority.

The seriousness of the growing threat is magnified by the fact that cyber-war technology is inexpensive and widely available to both nations and individuals. Even individuals or hackers acting in small groups can do serious damage. The tools and techniques for doing so are widely available on the Internet. Individuals no longer need be inordinately familiar with the intricacies of computer technology to be a threat[88].

The incentive to use technology is greatly enhanced by the fact that it may be very difficult, if not impossible, to trace the attack back to its source. Cyber-

86 Why the Dogs of Cyber-war Stay Leashed by Mark Rasch, 2003-03-24

87 Information War – Cyber-war – Internet-war by George J. Stein

88 http://www.thejakartapost.com/detailfeatures.asp?fileid=20050321.P03&irec=2

war may also be quite easily dissimulated as "accidents" within the infrastructure of the target country itself.

The Existing Texts

While the law regarding cyber-war is likely to rely on UN Charter principles to define the legal boundaries of cyber-space, there is nevertheless a need for modern international law to define more precisely the criteria used to distinguish which state actions are permissible. Technological change may even reveal contradictions among existing legal principles.

There are many challenges posed by cyber-war that existing international law does not cover.

Firstly, the type of damage that such attacks may cause may be rationally different from the kind of physical damage caused by traditional warfare. Bombs and bullets are visually destructive; however, the disruption of information systems may cause intangible damage, such as disruption of civil society or government services.

Secondly, the sovereignty of states is disrupted by the ability of technology to cross borders without hindrances. Sovereignty, a fundamental principle of international law since the Treaty of Westphalia of 1648, holds that each nation has exclusive authority over events within its borders. Radio waves or satellite signals, and the Internet, now allow individuals or groups to cross borders, while national legal authority generally stops at those same borders. The intangible violation of borders, that these signals may cause are not understood as traditional violations of sovereignty.

Thirdly, it will be harder to define the targets of cyber-war as military or civilian. The intangible damage the attacks cause may not be the sort of injuries against which the humanitarian law of war is designed in its protection of noncombatants.

Existing international law regarding cyber-war is sparse to non-existant. According to the Report of the International Law Commission to the General Assembly, the UN Charter normally prohibits international intervention through the use of armed force, but withholds comments on other, more subtle forms of coercion that do not involve a perceived threat of force. As force is too loosely defined, there is a great need to devise legal restrictions on the use of cyber-force.

The Loopholes

Future international law must adapt to the fastchanging nature of transnational communications systems[89]. The United Nations has an opportunity to focus on not only creating international law regarding cyber-war

89 Cyber-Space, The Next Battlefield By Jim Wagner

but also an organization that focuses on the issues, threats and problems cyber-war poses to the global community.

The great shortcoming of international law is that it lacks the power of domestic law. Not only is there no real legislature, there is also no compulsory jurisdiction, or enforcement system. International law is created by means similar to entering into a contract where the parties to the agreement, whether countries, organizations, or a combination of the two, consent to be bound by specific terms. As a result, the parties to an agreement will commit violations where they feel their state interests in taking a proscribed action outweigh the political and diplomatic consequences of breaking the law.

The problem in many cases, cyber-war included, is that it is unclear whether conduct is prohibited under the present framework. Often the legality of issues remains unresolved until one nation acts and the United Nations General Assembly or the Security Council responds to that act. Such a system is simply insufficient to regulate the use of information technology. A convention convened for the purpose of drafting a set of rules governing cyber-war is most likely the only way that a binding international doctrine on the subject will be enacted.

The question for such a convention is whether a nation's sovereignty is violated when an individual or a country accesses computer networks in another jurisdiction.

Article 2, Section 4 of the U.N. Charter prohibits, *"the threat or use of force against the territorial integrity or political independence of any state . . .* Article 39: *The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Articles 41 and 42, to maintain or restore international peace and security.* Article 41*: The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions* …..Article 42*: Should the Security Council consider that measures provided for in Article 41 would be inadequate or have proved to be inadequate, it may take such action by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such action may include demonstrations, blockade, and other operations by land, sea or air forces of the United Nations"*. These articles describe the conditions under which the Security Council may authorize the use of armed force.

Article 51 of the Charter describes the condition under which individual members, individually or collectively, may use armed force in self-defense, and stipulates that, *Nothing in this Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures to secure international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*

The question is whether cyber-war qualifies as either a use of force or an armed attack. Neither the Charter nor the International Court of Justice defines these terms. Hence, it is unclear what exactly constitutes an armed attack. The term has been construed to require the use of armed forces, force, or violence, as well as interference with a nation's sovereignty. Without clarification from the U.N., a member state cannot know whether it is legally justified in responding to a cyber-war attack. It would certainly be problematic for a nation under siege from a cyber-attack to wait for the U.N. to decide whether it can or cannot respond.

The United Nations Declaration on the Definition of Aggression is equally unhelpful. It provides that the U.N. Security Council can address acts of aggression, which are characterized as, *"the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State"*. The declaration enumerates a non-exclusive list of acts that qualify as aggression, including, "*invasion or attack by armed forces, military occupation, annexation by the use of force"* on a foreign state, *"the use of any weapon"* against a foreign state, and an attack on the armed forces of another state. It is difficult to say whether cyber-war constitutes aggression. Although the results of cyber-war are tangible in a physical sense, the act of indulging in cyber-war itself is non-physical.

The U.N. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States (*Non-Intervention Treaty*) prohibits direct or indirect intervention in the, *"internal or external affairs of any state. It* also provides that *armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic and cultural elements, is condemned"*. The major problem with the treaty is that it does not define intervention. It also gives no indication about which forms of interference constitute aggression warranting a response in self defense under Article 51 of the Charter.

International law regulates war on two fronts[90]: the conduct of warring parties toward each other, and the conduct of belligerents in relation to neutral states. Whether cyber-war can be characterized as an act of war is essential to determining the constraints that the international community will place on its wartime use. If cyber-war is an act of war, then the following principles will govern its use.

The fundamental principle of humanitarian law is that there are limits to the methods that can be used against adversaries during warfare. Warring nations must avoid inflicting even collateral civilian injuries on a belligerent's civilian population. This concept was originally codified in the St. Petersburg Declaration of 1868 which, *"recognized that the only legitimate object of war was to weaken an enemy's military forces"*. Civilians are not legitimate targets. Only military objectives may be targeted. They include those, *"which by their nature, location,*

90 www.bu.edu/law/scitech/volume6/Robbat.htm

purpose, or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, . . . offers a definite military advantage". Because of the concern over attacking proper objectives, humanitarian law[91] requires that nations use weapons that allow aggressors to distinguish between military and civilian targets. The problem is that both the military and civilians use many of the same information systems. Thus it is unclear whether these dual-use systems may legally be attacked.

For example, according to customary international law, it is legal for warring parties to cut off lines of communication. As such, action taken to destroy or inhibit the lines of communication between military systems would most likely be permissible because they are a major military objective; but weighed against the potential harms that civilians might incur, this proposition becomes debatable. For example, a virus that is unleashed on a dual-use system might inhibit both its military and civilian functions, causing great hardship to civilians.

Humanitarian law also requires the aggressor to abide to the principle of *proportionality* in considering whether its attack is justifiable. The principle mandates that attackers weigh the potential civilian damage that might result against the benefits to be derived from attaining the military objective. The principle requires that parties responding to attacks consider whether their use of force in response is proportional to the wrong. Whether this principle applies to cyber-war is important for two reasons.

Firstly, it creates difficult issues for information warriors who seek to attack dual-use targets. If the principle does not apply to cyber-war, attackers do not have to be concerned with civilian losses. Secondly, if cyber-war is covered, it will be difficult to weigh whether the type of response is appropriate. Can a nation use physical means to respond to a cyber-war attack? What are the implications of using cyber-war to respond to attacks that occur in the physical plane? These dilemmas must be resolved in light of the proliferation of cyber-war technology.

During times of war, belligerents may not pass through or use the territory of neutral states. Thus, if cyber-war is construed as an instrument of force, it is arguable that information warriors would be prohibited from channeling attacks through the networks of neutral states. Given the ephemeral and uncontrolled nature of the Internet, it is difficult to see how that interdiction can be exercised.

In the past, such use of a neutral's territory was confined to the physical realm. Cyber-war attacks take place in another dimension, however, and once again there is no indication that the current law will cover these attacks.

91 www.iwar.org.uk/law/resources/iwlaw/Ellis_B_W_01.pdf

The Suggested Solution

It can be argued that the use of cyber-war is an armed use of force and therefore invokes Article 2, Section 4 and Article 51 of the U.N. Charter, the Definition of Aggression, and the Non-Intervention Treaty. International law theorists have been reluctant to characterize cyber-war as such, but their hesitance is unfounded[92]. As technology has advanced, we have used machines as a more efficient means to carry out tasks that previously required use of human force in the tangible, physical sense. These innovations symbolize humanity's ongoing progression away from reliance on a physical means of carrying out force towards reliance on technology to achieve the same effect.

If a logic bomb can be detonated at a given time to severely damage computer systems, leading to subsequent physical damage, this is hardly different from an actual bomb on its way to a target. Each of these types of bombs is capable of causing the same amount of damage, may be detected before it blows, and should therefore be treated similarly.

A nation should not have to wait until a dormant threat comes to life as an attack in order to respond to it. No army officer would argue that he must wait for detected enemy forces lying in the tall grass of an open battlefield to attack before they can be eradicated. The same concept applies to dormant cyber-war threats. Thus, even attacks that have not yet manifested themselves should be considered armed uses of force. Once more, it is the intended result that is critical.

It is imperative that the new international paradigm characterize acts as either war, terrorism, espionage, or something not prohibited by international law, so that nations under siege can know whether, and to what extent, retaliation is justified. Only by focusing on the result, rather than on the means by which that result is effectuated, can such clarity be achieved.

The most challenging aspect of regulating cyber-war[93] will be the difficulty that victims will have in tracing the attack back to its source. Lack of accountability will encourage increased and reckless use of cyber-war. Thus, a new legal paradigm will effectively prevent, or at least limit, the use of cyber-war only if the repercussions of doing so are a sufficient deterrent when balanced against the gain sought by potential attackers. The seriousness of this threat indicates that the deterrents must be great indeed.

Terrorists might shut down an airport's control tower, causing many planes to crash, with resulting deaths in the hundreds or thousands. Such an act, though traditionally considered terrorism, must, in consideration of the potential extent of the harm, also be considered an act of war when sponsored by nation-states.

The same reasoning applies to state-sponsored espionage. Nations have been willing to tolerate a certain amount of such activity. The law frequently

92 http://www.psycom.Internet/iwar.1.html

93 Computers And War: The Legal Battlespace By Michael N. Schmitt,

takes a results-based approach and distinguishes between, for example attempted wire fraud aimed at a single bank, and an attempt to shut down the New York Stock Exchange.

In fact, because the damage that cyber-war can cause is comparable in many ways to the damage that may result from traditional physical means; the law must also agree to hold parties accountable for the negligent use of cyber-war. For example, if a nation's information warriors plant a virus that causes a navy plane of another nation to accidentally crash into its carrier, the responsible nation should not be able to claim it was an accident. The consequences of cyber-war technology are grave, and its negligent use should not be excused. The law must create severe penalties, including a possible damage repayment system, to deter nations from claiming ignorance[94].

The law should also require nations to cooperate in investigations, by allowing victim-states access to computer networks that may have been used to disguise the source of an attack. Refusal to cooperate with a reasonable investigation might be met with sanctions against that nation. In extreme situations, where there is strong evidence that the nation is shielding individuals who acted on its behalf, that evidence, combined with the refusal to cooperate, should be interpreted as an act of war.

As cited by World Federation of Scientists Permanent Monitoring Panel on Information Security in August 2003 in its Recommendation 3[95]: "*Cyber-crime, cyber-terrorism, and cyber-warfare activities that may constitute a breach of international peace and security should be dealt with by the competent organs of the UN system under international law. We recommend that the UN and the international scientific community examine scenarios and criteria and international legal sanctions that may apply.*"

Cyber activities that constitute deliberately hostile actions[96] by nation states may threaten international peace and security, and yet elude penal sanctions under current legal frameworks or a future Law of Cyber-Space. One consideration is that, under certain circumstances, the international doctrine of sovereign immunity protects nation states against legal actions. This protection could conceivably extend to offensive cyber actions taken by nation states. Other concerns relate to the lack of international cooperation on a global scale, and technical considerations regarding the inability to effectively track and trace Internet communications.

The nations of the world must come together in a convention to confront the threat that cyber-war presents. The conclusion that must be reached is that cyber-war is eqivalent to the use of force as defined by United Nations documents.

94 "Cyber-attacks and International Law" from Survival, Autumn 2000, by Grove, Goodman, Lukasik
95 www.apdip.net/documents/access/ security/wfs_cybersecurity082003.pdf
96 Lipson at 3, http://www.cert.org/archive/pdf/02sr009.pdf

CHAPTER 13. DISTANCE CONTRACTING

GENERAL CONSIDERATIONS

The Problem

The Internet has affords new and exciting channels of distribution and marketing opportunities to existing businesses. The term covers computer-to-computer processing of a growing variety of transactions, ranging from electronic data interchange ('EDI')[97], the well-established handling of business-to-business purchase orders, invoicing, remittance notices and other routine documents, to electronic payment systems, credit cards and consumer sales of goods and services.

Electronic commerce is increasingly used to mean Internet commerce. The Internet's size, growth rate and ease of access open up immense market opportunities for large, medium and small firms. Businesses throughout the world are transmitting and exchanging commercial information, software, and services electronically, setting the stage for a revolution in the way commerce is transacted. Fuelling this revolution are the substantial efficiencies to be gained in the transition from paper-based to electronic data exchange mechanisms.

Electronic Data Exchange technologies, such as electronic data interchange (EDI), have long held the promise for a less burdensome, more highly efficient system for transacting global business, as well as the possibility for creating new channels for distribution, sales, and licensing.

The availability of Internet technology on a worldwide scale is commonly seen as the decisive element in the developing information society, and essential for new business opportunities in the world. Despite the fact that there is still a lot of legal uncertainty about the validity and enforceability of contracts concluded online on the Internet, e-commerce is a booming and fast growing phenomenon. Businesses have pressed on with it due to the need to enter the market as early as possible.

The global and simultaneous exposure of any website on the Internet to virtually any place in the world goes beyond any previously known method of mass communication and/or individual communication between vendors and buyers. In essence, Internet technology allows both of them to communicate with each other transparently and simultaneously, in real-time, and interactively.

Electronic commerce is difficult to define because of the diversity of the Internet marketplace and the rapid evolution of relationships between marketplace participants. One possible definition could be the convergence of electronic communication and digital information processing technology in support of the core business functions[98].

97 www.business.com/directory/Internet_and_online/ ecommerce/electronic_data_interchange_edi/
98 www.bakerInternet.com/ecommerce

Electronic commerce may ultimately be best understood in terms of the infrastructures necessary for its operation:

- technological infrastructure, or telecommunications networks Internet service provider connectors; and computer, phone, or other electronic end-use devices
- process infrastructure, or electronic payments systems; distribution and delivery mechanism
- code infrastructure, or technical protocols to ensure interconnectivity; along with the laws and regulations needed to define relationships among participants.

Market analysts have identified various categories of participants in E-Commerce Transactions. They are Business-to-Business (*B2B*), Business to-Consumer (*B2C*), Business-to-Employee (*B2E*), and recently also Consumer-to-Business (*C2B*) relationships, the latter referring, in particular, to websites channeling group buying, public procurement procedures, and tenders, etc.

The distinction between these different groups is, obviously, essential where consumers are involved, and raise specific legal issues concerning consumer and data protection. Any E-Commerce Transaction can be described as either an Indirect E-Commerce Transaction or a Direct E-Commerce Transaction. An Indirect E-Commerce Transaction is where a Vendor and a Buyer conclude a contract via the Internet, but perform their contractual obligations (for example, the delivery of the goods and/or the performance of the services, and payment of the purchase price) by means other than through the Internet (off-line). The purchase of tangible goods will, therefore, always constitute an Indirect E-Commerce Transaction. The supply of tangible goods in connection with the delivery of a service (for example, the delivery of an airline ticket to a Buyer) will also constitute an Indirect E-Commerce Transaction. A Direct E-Commerce Transaction is where a Vendor and a Buyer not only conclude the contract, but also perform all their contractual obligations via the Internet on-line. Such a Direct E-Commerce Transaction is only possible if the goods purchased are intangible or the services are performed exclusively through the Internet or by other electronic means. For example, the purchase of software, films, music or information (such as the contents of a book) which are downloaded to the Buyer via the Internet will constitute a Direct E-Commerce Transaction.

Apart from its relevance under international trade rules and tax laws, it is generally more a question of theory whether Direct E-Commerce Transactions can be regarded as involving the supply of virtual goods (which is the more common view, for example, in the United States), or whether all Direct E-Commerce Transactions should be regarded as the provision of services within the meaning of information society services (as seen defined by the EC[99]).

99 http://www.bna.com/

The Existing Texts

UNCITRAL Model Law[100]

As a result of the growth foreseen for ecommerce as an international phenomenon the United Nations Commission for International Trade Law drew up a model law to be used world wide by legislatures in order to promote legal unity as far as possible in regard to e-commerce law.

UNCITRAL Model Law on Electronic Commerce – (December 1996, modified June 1998) establishes rules that define the characteristics of a valid electronic contract and that govern the admissibility and evidential weight of electronic evidence in legal disputes over the validity of a contract; rules are based on a general rule of nondiscrimination in that information should not be denied legal effect, validity, or enforceability solely on the grounds that it is in electronic form.

The UNCITRAL Model Law on Electronic Commerce (*Model Law*)[101] is a generic law which can be extended and enhanced by individual countries should they so wish. In devising the Model Law, UNCITRAL had set out to develop rules that could be used in all countries regardless of their technological proficiency or the legal framework under which these countries operated. This automatically preempted the possibility of developing *sui generis* rules that are sensitive to the full possibilities of digital technology. The Model Law provides generally[102] that electronic communications should be given equivalent legal effect to paper-based communications and specifically addresses how certain types of electronic communications could substitute for existing paper-based means of satisfying requirements of writing, signatures and contract formation. These model laws have served as the basis for legislation enacted in several countries.

THE WORLD TRADE ORGANIZATION

WTO has defined E-Commerce as*: the production, distribution, marketing, sale or delivery of goods and services by electronic means* (WTO Declaration on Electronic Commerce dated 25 September 1998).

EUROPEAN UNION

The EU has created an extensive legal framework addressing various issues in relation to information society services, and, in particular, their relevance to e-commerce. Among the various detailed regulations, are the E-Commerce Directive[103], the Electronic Signatures Directive, the Distance Selling Directive and the Proposed Copyright Directive.

100 United Nations Commission on International Trade Law, Thirty-sixth session Vienna, 30 June-2003

101 http://www.uncitral.org/english/texts/electcom/ml-ecomm.htm

102 United Nations Commission on International Trade Law Working Group IV (Electronic Commerce) Forty-third session, New York, 15-19 March 2004

103 www.europa.eu.int/ISPO/ecommerce/legal/documents/2000_31ec/2000_31ec_en.pdf.

The European Commission has defined E-Commerce as: "*Any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services*".

In May 2000, the EC adopted a Directive on Certain Legal Aspects of Electronic Commerce. This directive is intended to address some of the legal uncertainties relating to contracting online and to establish a single market for electronic commerce within Europe. This directive provides a legal framework for Information Society Services (ISS). The E-Commerce Directive is without prejudice to other EC and national legislation with respect to contracts, whether through electronic communication or otherwise. In particular, Directive 97/7/EC on the Protection of Consumers in Respect of Distance Selling and Directive 93/13/EEC on Unfair Terms in Consumer Contracts remain applicable after the implementation of the e-commerce directive in the national law of the member states. In addition to these directives, a number of other directives also remain fully applicable. Moreover, the member states' national contract law continues to apply.

In the European Union, the enforceability of electronic transactions is governed by the Electronic Signatures Directive adopted in 1999, and the Electronic Commerce Directive adopted in 2000. The European Union Electronic Commerce Directive does not require consent of the parties, but instead requires that information society services (for example, sellers of goods online) provide specific information to the other party regarding the transaction. Such information includes a comprehensive and unambiguous statement as to the technical steps to follow to conclude the contract, whether or not the concluded contract will be filed by the service provider and where it will be accessible, the technical means for identifying and correcting input errors prior to the placing of the order, and the languages offered for the conclusion of the contract. The service provider is also obligated to acknowledge receipt of the purchaser's order without undue delay and by electronic means, and is required to make available to the purchaser appropriate, effective, and accessible technical means allowing him to identify and correct input errors prior to the placing of the order.

ASIA

Frenetic activity in the past few years have ensured that lawyers and policy makers specializing in information technology law are kept busy monitoring developments that are taking place in many parts of Asia. Examples of legislation passed or sought to be passed in Asia [104] include Australia's Electronic Transactions Act 1999, Broadcasting Services Amendment (On-Line Services) Act 1999, Privacy (Private Sector) Bill and the Copyright Amendment (Digital Agenda) Bill 1999; the Republic of Korea's Electronic Transaction Basic Act; Singapore's Electronic Transaction Act 1998; Hong

104 www.apdip.Internet/asian-forum

Kong Electronic Transactions Ordinance 2000; Japan's Draft Bill Concerning Electronic Signatures and Certification Authorities and the Law Partially Amending the Trade Mark Law; Malaysia's Malaysian Communications and Multimedia Commission Act 1998, Communications and Multimedia Act 1998, Digital Signature Act 1997, Computer Crimes Act 1997 and Telemedicine Act 1997; the Philippines' Electronic Commerce Act; and India's Information Technology Act 2000.

USA

In the US, the enforceability of electronic transactions is primarily governed by the Electronic Signatures in Global and National Commerce Act (*E-SIGN*), a federal law enacted in 2000, and the Uniform Electronic Transactions Act (*UETA*), a uniform state law that was finalized by the National Conference of Commissioners on Uniform State Laws (*NCCUSL*) in 1999 and which has now been adopted by 40 states.

Under these laws, a web-site must have a clear statement of terms and conditions that establish when a contract is concluded. Typically, a United States based company that puts images of its products online is making an offer to sell those products to consumers who click on the products and add them to a shopping cart. Once the products are added to the shopping cart, the consumer is indicating his acceptance of the offer and by providing payment information is acknowledging an agreement to pay for the product and any associated shipping costs.

The Loopholes

The following seem to be the major concerns that need to be addressed by the law to provide greater consumer confidence in e-commerce:

- The security of confidential information passed on to cyber-businesses, especially payment information such as credit card numbers or banking details.
- The security and confidentiality of private information passed on to cyber-business such as name, addresses and other profiling details which may be passed on to other businesses or persons and could lead to unwanted e-mail and solicitations (spamming).
- The validity and binding nature of virtual communications and agreements concluded on the Internet.
- The legal system applicable to a particular contract. The law is still territorially based and organized.

With the globalization of commerce and the growth and expected growth of e-commerce, the flexibility and the ability of the law to deal with contracts concluded in cyber-space are severely tested. There is a widely held belief that the law is slow moving and unable to properly cope with the demands of modern technology. In fact, despite the ancient history of the law of contract,

it is surprisingly resilient and flexible and therefore able to deal with new phenomena without any major changes.

The main differences are found in the fact that:

- The contracting parties never meet face to face as in conventional transactions. Superficially this is also true of all distance contracts where communications such as a letter, telex, telephone or fax is used. Except for the telephone, none of these forms of communication however is as inter-active as electronic communications. Even telephone communication cannot be as graphically attractive or informative as an inter-active website.
- International borders have been eroded and transactions can span the globe without any difficulty or cost implications. This causes uncertainty about the applicable legal system. Until the advent of e-commerce very few consumers conducted any international transactions. Although the conclusion of the international contract has become easy, performance is often constrained by the physical world and enforcing ones rights when something goes wrong can become difficult and expensive.
- Sensitive personal information needs to be sent to complete strangers who superficially have only a virtual existence. It is psychologically much easier and comforting to divulge sensitive information to someone in person than sending it off to a faceless impersonal entity in cyber-space.
- Part or the whole transaction may take place automatically, without human interference. In all other forms of contracts a conscious human decision is made whether to make the offer or accept the offer, whereas in cyber-trading one or both ends may be automated. In many electronic data interchange transactions the human intervention stops with the programming of the system or during periodic spot checks, but individual transactions are never interfered with.

As the whole transaction takes place virtually there is not a necessary physical proof of the transaction is absent. The proof that does exist is electronic, and is capable of easy manipulation and therefore not very trustworthy[105]. This fact further undermines consumer confidence in the medium.

The law of contract has developed over time on the assumption that the contracting parties are in the presence of one another. Communications from a distance are the exception rather than the rule and special rules have been developed for these situations.

A contract becomes final and binding once there is consensus or agreement between the parties. Consensus is reached once both parties have

105 general.rau.ac.za/infosci/www2001/abstracts/eiselen.htm

the same rights and obligations in mind and have agreed to them. This is the so-called subjective or will theory of consensus.

In web-trading the offer may either be contained on the website if that is the intention of the e-business, or a website may simply contain an "invitation" to do business. Any order sent to the website, will constitute a purchase offer which may be accepted or rejected by the website. Thus only the "confirmation" of the offer will usually constitute an acceptance by the web-trader of the offer made by the client. However, if the website offering is itself viewed as a valid offer, the mere placement of the order by the client will constitute an acceptance.

In terms of the usual rules applicable, a contract comes into existence at the time and place that the dealer receives and takes subjective notice of the acceptance. In terms of this construction an Internet contract in the usual case will become final and binding once that confirmation is received and viewed by the client. Acceptance must come to his subjective notice. This creates a problem where the conclusion of the agreement takes place automatically without human intervention.

An approach used in many jurisdictions which is worthy of consideration is the receipt theory. In terms of this approach the contract is deemed to be concluded at the time and place that the acceptance reaches the dealer and is received by it. It is fairer to both parties than the postal rule in that the inadvertent risk of a misdirection of the message completing the transaction is placed on the sender of the message. The sending party has more control over the message than the receiving party and the risk should therefore be borne by the former. It is also much fairer than the usual rule in that the latter is open to abuse by the dealer. By refusing to open an e-mail, or letter or message, the dealer can delay taking notice of the content of the message or letter and so delay or even prevent the conclusion of the contract. This becomes especially important where acceptance is subject to specified timeframes. The reception theory makes this kind of manipulation impossible because it relies on objective facts, namely receipt.

A problem that may be encountered in the application of standard terms and conditions in the international context is that there are many countries where consumer legislation regulates the validity of standard terms. Unconscionable or unfair terms may be deemed unenforceable or invalid in terms of such legislation because they are one-sided, oppressive, unusual or unexpected. Even though such legislation may apply only in the country of origin, if the proper law of the contract assigns that legal system as the applicable legal system or where the contract has to be enforced in that country, such legislation will apply.

The point of departure in respect of formalities is that there is freedom of form except where common law, statute or the parties themselves require formalities such as writing or signature as mandatory. Where there is a

mandatory requirement, those formalities must be complied with before a contract will come into existence.

Writing is prescribed as a formality for the following reasons:

- to provide legal certainty about the contents of the agreement between the parties;
- to provide objective proof that cannot easily be refuted by either party.

Writing has traditionally been associated with paper-based applications where words are typed or printed on paper or similar media. Whether the words created on a computer screen will be viewed as writing is still not settled in the law of many countries, but there seems to be a consensus under writers that presentations of words on a computer also constitutes writing.

The problem with cyber-writing however is that unlike writing on permanent media like paper, what is transfixed on the floppy, CD Rom or hard disk has to be further processed and does not constitute writing in itself. Due to its transient nature, cyber-writing has lost much of its original evidential value unless it is coupled with other safeguards ensuring that the original text remains unchanged.

The evidential value and weight is another problem that should be taken into account when dealing with computer evidence, but it should in itself not become a reason to disallow that evidence. This seems to be the approach followed in most Western orientated legal systems. The fact that electronic information may easily be changed or manipulated without apparent trace causes some of the concern about accepting computer generated evidence without further examination.

A closely associated problem deals with the question of originality that is usually required in the law of evidence. It is not possible to talk of an original document in this context, but is suggested that the sensible approach to this issue is to simply accept copies such as printouts, but to scrutinize the circumstances under which such printouts were made in order to establish reliability.

Since time immemorial signatures have been used for the following purposes:

- Identification: to prove the identity of a party. The signature on the document can usually be used to identify the party affixing that signature to the document.
- Attribution: to connect a specific person to a specific document. It is important to link the signature to a specific person in order to make that person liable for any obligations created in the document or to entitle a person to rights created in the document.
- Assent: to prove that parties assent to the document, binding a particular party to the contents of that document. A signature to a contract usually indicates the agreement of that party to the contents

of the document. Where a party fails to read the document but nevertheless signs it, the warning rule will ensure that the party is bound to the information contained in the document. The risk for not reading the document rests with the signatory, unless there was a duty on the other party to alert the signatory to unusual or oppressive terms in the document.

- Authentication: to indicate and ensure the reliability of the document and the information it contains. By signing a particular document or set of information, the signatory confirms that that is the relevant document, especially where a document has gone through a number of drafts. In the case of a witness signing a document that signature usually authenticates the signature of either or both parties.

In most legal systems a signature is usually defined with a paper document as point of departure, namely a mark or writing affixed to a document which identifies it as the act of the party or is intended to be a signature by the party. An electronic signature affixed to an electronic document would probably not qualify as a signature even if it is just as effective as an original paper-based signature. Legislation providing for the validity of electronic signatures is therefore necessary.

Thus, moving transactions to an electronic environment has two important consequences. Firstly, in many cases it is difficult to know when one can rely on the integrity and authenticity of an electronic message. This, of course, makes difficult those decisions that involve entering into contracts, especially for significant transactions. Secondly, this lack of reliability can make proving a case in court difficult at best. For example, if the defendant denies making the signature that is appended to an electronic document, it may be virtually impossible for the plaintiff to prove the authenticity of that electronic signature in the absence of additional evidence.

If e-commerce is to reach its full potential, however, parties must be able to trust electronic communications for a wide range of transactions [106], particularly ones where the size of the transaction is substantial or the nature of the transaction is of higher risk. In such cases, a party relying on an electronic communication will need to know whether the message is authentic, whether the integrity of its contents is intact [107], and whether the relying party can establish both of those facts in court if a dispute arises.

One of the biggest challenges facing international bodies that are interested in e-commerce is the issue of cross border enforcement of rights and obligations. The scope for conflict between counterpart legal systems is immense. It is not just the replacement of paper documents which makes such problems likely, but the emergence of virtual businesses operating effectively

106 profs.lp.findlaw.com/signatures/signature_5.html

107 www.ucsc.cmb.ac.lk/pdc/resources/ Ecommerce%20Security%20&%20Legal-%20IITC.pdf

from jurisdictions which, save for the location of the source server and perhaps the stated governing law clause, have no real or substantial connection with the parties to the contract or its subject matter.

Such jurisdictions may well be remote from the parties, the products and the place of performance and may be relatively more inhospitable in legal terms to foreign litigants compared to the litigant's home jurisdiction. In such cases, whilst consumers may be well placed to obtain orders in their home jurisdictions, exporting such orders and enforcing them in the server jurisdiction may be fraught with difficulty.

The Suggested Solution

Standard business terms must be implemented to ensure that a clearly defined, legally binding relationship is created. This will set expectations, manage risks and keep potential liability capped at a reasonable level. Normal contract law applies although the characteristics of an electronic transaction appear to innovate on traditional contracting mechanisms. The basic rules of contract law should apply to any transaction over the Internet in the same way as any other transaction.

A contract is formed if one party accepts an offer, which is made by another party to sell something, provided that both parties intend their transaction to be legally binding. This can be electronically concluded. Terms must be brought to the attention of the other party before they agree to purchase the goods or services. Ideally the buyer should be forced to scroll through the terms and conditions. At the very least the buyer should have to click to confirm that the terms and conditions are accepted before concluding a transaction.

Certain terms will take on greater significance when doing business online. Since the website may be accessible anywhere, a term stating which country's laws will govern the contract, and where any disputes will be dealt with is essential.

If someone anticipates doing business with customers in a number of different countries, one should be aware that the specific clauses of the law of an individual country may have some overriding effect on general terms.

Business-to-consumer sales online are usually technically simple, often only requiring the completion of an online form. The legal requirements should not be underestimated. It is important that, before a deal is concluded:

- the customer has seen, read and accepted the terms and conditions
- the customer has specified a delivery address
- the ordered goods and the price to be paid are clearly identified.

In the business-to-business environment, the size of an average contract is frequently substantial and therefore requires even greater and more detailed attention. Electronic signatures are likely to be of greater significance in B2B contracting than in B2C transactions.

A certification authority is a trusted third party willing to verify the identity of a signatory party with a given key and to issue certificates confirming that identity. Certification authorities can impose limits upon the use of an electronic signature, for example, by indicating the value of transactions for which it is valid and restricting their financial liability to that limit.

This makes the role of certifying authorities extremely important. Electronic signatures when combined with a certificate from a certification authority will: (a) be legally equivalent to a handwritten signature, and (b) be accepted as evidence in legal disputes.

A set of terms and conditions to govern the use of a web-site must be established, irrespective of whether the user buys any goods or services. Such terms and conditions should cover:

- copyright and trade marks - specify the content that is subject to copyright protection and identify registered trademarks
- use of the site - state clearly what may not be done.
- use of links - make users aware that you are not responsible for other websites visited through links posted on your site
- restrictions on linking – to be clear that others cannot link to the site without consent
- security assurances - evidence of data security should be provided, especially where payment is involved.

An appropriate use of disclaimers helps avoid potential disputes in the future and clearly defines the intentions of the online business as well as the rights and responsibilities of its customers. Web-sites must also have an appropriate privacy policy explaining what personal information is collected and why.

The same level of protection provided by the laws and practices that apply to other forms of commerce should be afforded to consumers participating in commercial activities through the use of global networks. The goal of reaching at least a similar level of protection should therefore be preferred

New breaches and threats in consumer protection call for new protective rules: the protection should be adapted to the technological evolution where the consumer is placed in new situations and is faced with new threats. In order for this to be effective contractual parties must be bound by the same obligations as are applied to a common commercial contract. Violations through fraud, forgery etc, must be punished accordingly with similar fines and imprisonment. These regulations would be ineffective if the states do not implement these principles on a domestic level and do not cooperate internationally in their implementation.

ELECTRONIC PAYMENTS

The Problem

Payment is a key element of electronic contracting. In lieu of credit cards, electronic money (e-money)[108] is increasingly used in contracting over the Internet. E-money can be best conceived as a digital form of cash money and it is used primarily for limited value payments. The monetary value is stored either on a chip card or in a software program. Unlike credit cards, the use of electronic money is not subject to prior authorization from a bank or any other third party.

The major issue in electronic payment is one of security: Confidence in electronic commerce will only develop when adequate security is provided with regard to payment on the Internet. Credit card numbers and expiration dates are all too often disclosed over the network without the back-up of a sufficient and reliable security system.

This lack of security is one of the reasons why consumers are reluctant to make payments on-line and thus to buy goods or services over the Internet. As long as the mere communication of the apparent number on the payment instrument suffices to engage a transaction, electronic transactions remain insecure. Moreover, security is necessary at two different stages: first, during the transfer of the information over the network; and second when the payment data is stored so that the data transmitted should not be accessible to unauthorized third parties.

The holder may not be held liable for payments made without either his physical presence or electronic identification having taken place; the simple use of a confidential code, or similar means of identification, is insufficient to engage his liability. The security of each payment system should obviously be described in words understandable to every consumer. Thus, providers should pay attention to the given information regarding the referred technique to and its consequences. Information should also focus on the related fees, charges or handling costs incurred by the use of a particular mean of payment. Until a higher level of security[109] and a better understanding of the risks for both consumers and businesses is achieved,, person-to-person payment systems will be favored.

The Existing Texts

Recent years have seen the emergence of what has been described as the third great age of payments, the first of these being that of cash payment, the second that of the paper based payments, and now a third great age of electronic funds transfers.

---

108 Peter Spencer - Regulation of the payments market and the prospect for digital money

109 Justin McCarthy - Consumer Protection in Contemporary Electronic Payment Systems:- A Familiar Wolf in Digital Clothing? -2002

As a result of innovative advances in computer technology, the financial services industry in the new millennium has been marked by an extraordinary level of growth in new types of payment facilities. These new electronic payment methods, as outlined in the UNCITRAL Legal Guide On Electronic Funds Transfers, are, *"a funds transfer in which one or more of the steps in the process that were previously done by paper-based techniques are now done by electronic techniques"*. Thus they include card based systems, the most popular of which are ATM (Automated Teller Machines), EFPTOS (Electronic Funds Transfer at Point of Sale), credit cards, and on-line banking from home. Fast and efficient payment methods such as these are of unquestionable benefit to all who use them. The advantages of real time funds transfers, as many of these payment methods offer, give greater financial control and access to both the issuer and the user of such methods.

The rules governing money transfers were drawn up when tangible coins and banknotes were the main forms of money. With money passing into electronic transfers, the existing law needed to be modified in relation to electronic funds transfer. Commentators agree that multinational actions undertaken by the EU, UNCITRAL, the OECD, as well as national undertakings by Denmark and the US, indicate a recognition of consumers' concerns in this area and the need for protection. However, disputes still exist regarding how best to protect consumers: mandatory legislation, or voluntary compliance with recommendations and codes of practice. Legitimate arguments have been advanced in favor of both of these options. The major argument in favor of voluntary compliance is that the relative novelty of electronic payment methods and future progress and innovations could be stifled by excessive regulation. On the opposite side, the major argument to be made in favor of mandatory legislation is that compliance would be enforceable and thus consumers would be better protected.

Different decisions have been taken in this debate around the world. The US opted for mandatory legislation through the enactment of The US Electronic Funds Transfer Act 1978. By contrast, Australia and the EU opted for what has been described as a soft law approach, in the form of recommendations and codes of conduct. In the EU, the first set of recommendations was the Recommendations to Payment Card Issuers. These recommendations were aimed to establish minimum standards for consumer protection in the area of customer activated electronic banking. While these recommendations would offer much increased consumer protection if implemented, they had many notable deficiencies. The most important of these is that they only applied to card–based systems. Thus other electronic payment methods such as home-banking and emergent digital methods, such as e-Purse[110], were not in the ambit of these recommendations, and so consumers

110 http://www.murdoch.edu.au/elaw/issues/v11n2/bollen112nf.html

using these methods continued to go unprotected. Other deficiencies with these recommendations included the failure to deal with some important consumer protection issues such as slanted advertising and confidentiality.

The European Credit Sector Association's (ECSA) response to the introduction of the 1988 recommendations was to produce a code of best practice. While the code was based on the 1988 recommendations, not all the recommendations were acted on. While this code did succeed in its aim to forestall the imposition of a European directive in the area, it has been criticized for two major reasons. The first of these is criticism for a low level of compliance. The second is that unlike the 1988 recommendations, the code fails to redistribute the balance of power between the financial sector and the consumer.

In 1997 the EU addressed some of the deficiencies highlighted in the 1988 recommendations by adopting new recommendations concerning the transactions by using electronic payment instruments. These new recommendations imposed a basic structure on all electronic payment systems across member states. These recommendations are seen as a substantial step forward with regards to consumer protection. They cover important consumer issues such as the settlement of disputes.

In 1989 the UK produced a report, The Banking Services Law and Practice Report (the Jack Report). This report describes the situation which exists where the banks, given the current legal vacuum have used their stronger bargaining position in imposing one-sided terms and conditions on customers. The report says that such an attitude is widespread and leaves the consumer with no choice but to accept such contracts if they want to avail of the benefits of electronic payment methods. A similar situation exists in Ireland, with consumers being forced to accept one-sided terms and conditions. Both in Ireland and England the only recourse open to consumers is to initiate legal proceedings under The Unfair Terms in Consumer Contracts Regulations 1995.

The Loopholes

Many legal issues arise as digital money becomes more prevalent. Given that most digital money will be global in the sense that the Internet will facilitate its movement or use outside its issuing jurisdiction, the lack of legal uniformity between countries raises many policy issues. For instance, who has the liability if a failure does occur in a particular digital money system because of fraud or for some other reason? When digital money payments are made across national borders, who has jurisdiction? Does digital money violate the monopoly rights of central banks to issue money? May a central bank issue digital money? Do non-bank issuers of digital money need to be regulated, and if so, who should be the regulator? Who is going to determine if the clearing organizations have sufficiently robust and fraud proof systems?

Another major issue concerning the regulation is the lack of compliance. It appears that mandatory regulation is needed to control the relationship created by electronic payment methods. Firstly, payment method issuers have a dominant position and so they can impose almost any terms and conditions that they wish on consumers. Secondly, the financial institutions are strong and powerful enough not to have to comply with codes of conduct and recommendations. Thirdly, it is clear that the measures designed to protect consumers must have legal force and enforceability if they are to be effective. The enactment of clear legal guidelines would represent an authoritative solution to the consumer protection issues.

For Business to Business transactions, many overseas customers use credit cards for online purchases, but credit cards are not a universally common method of online payment. For example, regulations in some countries hold cardholders liable for fraudulent charges, other countries are culturally cash-based, and others simply do not like credit.

Credit cards carry risks. Charge backs can be very costly for online exporters. Common charge back reasons are: fraud, disputes over the quality of merchandise, non-receipt of merchandise, or incorrect amounts charged to a card. Companies accepting online credit card transactions should be knowledgeable about the policies of the card issuing institution toward charge backs.

Account to Account transfers, in which money is transferred electronically between the customer's and the merchant's bank, are popular in many countries. A2A transactions offer the advantage of occurring in real time and of reducing the potential for fraud and charge backs.

There are many companies offering Person to Person services, in which funds are sent electronically to a third party, which in turn deposits the funds in the merchant's account. An example of a P2P service provider that conducts cross-border transactions is PayPal[111]. PayPal lets anyone with an email address securely send and receive online payments using a credit card or bank account. PayPal will also conduct currency exchange, allowing the customer and merchant to operate in their preferred currency. Other P2P providers, such as Western Union's BidPay, accept a credit card payment from the payer and then send a money order to the payee. Internationally, P2P transfers have come under some degree of scrutiny, so it is advisable to consult with a Commercial Service officer in the country you are targeting before deciding on a particular payment mechanism.

The Suggested Solution

In recent years, the triple threat of terrorism, identity theft and internal fraud, has increased the tension between the need for heightened security and

111 www.paypal.com

the demand for low cost and efficiency. Satisfying both of these requirements calls for a multi-faceted approach, beginning with a candid assessment of risks and including both robust technology, and a rigorous training of employees and other users. Moreover, the compliance effort must be ongoing and continually adapted to new threats. Yet numerous polls show that while large businesses are concerned about information security, it is less clear that they have expended the money, time and executive attention required to comprehensively address security risks. Therefore, electronic payments and transactions systems will have to continue to seek compromises between the need for security and the demand for convenience, rather than completely satisfying either or both. Which imperative prevails at any moment is likely to depend on the intensity of security breaches and threats that have captured recent headlines.

If businesses can continue to highlight the advantages of convenience, lower cost and reliability, new electronic payment products will become ubiquitous, or at least prominent, replacements for cash, checks and credit cards. From a legal perspective the fundamental point is that the appearance of new alternatives to the traditional payments systems raises a new question: is it feasible to allow a nation's payment system, for example money, to be controlled by an amalgam of divergent commercial organizations? Before the appearance of new and, to some extent, less regulated electronic payment systems in the 1990's, regulators did not have to ask themselves this question. To the extent that they pay heed to this issue now, there is a possibility that laws will be changed to accommodate the new systems. In this process, one challenge will be to determine what guarantees, resources and procedures are necessary to transform the new payment systems from novelty to reliability. The core of the problem is the fact that the future law must bind the contractual parties by the same obligations as relate to a traditional commercial contract and means of payment. Consequent violations through fraud, forgery etc, must be punished with fines and imprisonment. Due to the cross border feature of Internet and the e-commerce states must implement this recommendation at their own domestic level, and coordinate this through the international cooperation mechanism.

TAXES

The Problem

The emergence of e-commerce has sparked a revolution that promises to transform the way businesses and commercial transactions are conducted throughout the world.

The rapid growth rate of e-commerce has sparked a debate about how governments should regulate these transactions, and one aspect of this debate focuses on the issue of taxation. Internet entrepreneurs advocate the limited involvement of government so that competition and consumer choice can allow e-commerce to continue its growth unfettered. Meanwhile, as sales conducted via Internet continue to skyrocket, state and local governments have grown concerned about a loss of tax revenue and autonomy.

As the Internet makes way for new business transactions through its complex telecommunications network, a single definition for e-commerce becomes elusive. The Office of Tax Policy at the US Department of Treasury defines e-commerce most broadly as any transaction that occurs with the facilitation of electronic tools and techniques. The Internet Tax Freedom Act, on other hand, more narrowly defines e-commerce as, *"any transaction conducted over the Internet or through Internet access, comprising the sale, lease, license, offer or delivery of property, goods, services or information, whether or not for consideration, and includes the provision of Internet access"*. Various international bodies, such as the OECD and the World Bank, offer alternative definitions.

Regardless of how narrowly or broadly e-commerce is defined, e-commerce occurs in various forms and between various entities in the market. It is necessary to consider these various forms in order to understand the implications for taxation. E-commerce can be categorized in two ways: (1) business to consumer (B2C) and business to business (B2B); and (2) tangible and intangible, or digital goods.

State and national governments traditionally have relied on a diversity of taxation methods. These traditional methods of taxation represent the tools available to government officials in the e-commerce environment. They include income taxes, consumption taxes such as sales or value-added taxes, excise taxes, and international tariffs.

VAT is probably the most talked-about electronic commerce taxation issue. The question is whether a web-based sale is taxable and if so, what jurisdiction, if any, may collect the tax. Many web-based sales are made free of indirect taxes, and as a result tax authorities are losing out on revenue[112].

Tax administrators are therefore very concerned about the challenges presented to taxation systems by globalization and the growth of electronic commerce. However, these international developments hold out new opportunities for the entire global community. Tax administrators are faced with challenges to existing tax laws and principles. The Internet in particular has potential to increase tax competition, by making it easier for multinationals to shift their activities to low tax regimes. On the other hand, taxpayers will want to take advantage of the increasing opportunities presented by these developments. Taxation should not be a barrier to the growth of e-commerce.

112 www.economist.com.na/2004/22oct/10-22-10.htm

Electronic invoicing (e-Invoicing) is one of the building blocks of the new e-World. The invoice is often considered to be the most important document in commercial trade. From a VAT point of view, the invoice is the primary document that evidences the supplier's obligation to charge VAT, and more importantly, also substantiates the customer's entitlement to VAT recovery.

The Existing Texts

Two types of taxes are commonly charged on Internet sales, Value Added Tax (VAT) in Canada, Europe, and some other areas, and sales tax, levied by some states, counties, and cities in the US). A merchant who has a business in only one state of the US is currently not required to collect sales tax on sales made outside his state. Members of the European Union [113] are currently required to charge VAT on all sales.

USA

In 1998, the US Congress passed the Internet Tax Freedom Act. Although this did not prohibit taxing Internet transactions, it did prohibit discriminatory taxes. In addition, it did establish a moratorium on Internet access taxes, and this has now been extended through 2007. Merchants are not required to collect sales taxes from out of state consumers. The Supreme Court ruled that merchants only need to collect taxes if they have a physical presence, known as a nexus, in the state and this is true for all mail order sales. Some states require consumers who purchase by mail order to pay a "use" tax, which covers the sales tax that would have been paid. In most cases, monitoring is nearly impossible, so use taxes are rarely enforced. Some exceptions are , products that are to be registered (for example automobiles), and purchases by large businesses (since these businesses are audited for tax compliance).

Some large Internet retailers are presently collecting sales tax on sales to buyers in any state that has a sales tax, in exchange for an amnesty for the retailer on any past uncollected taxes. At present, 34 states and the District of Columbia are agreeing to the Streamlined Sales Tax Project (SSTP), designed to simplify tax collection for merchants. After these states approve the SSTP, the US Congress must also approve it, but this may be a year or two away. Initially, it is expected that only larger online merchants will be required to collect sales taxes for sales in other states, though eventually, this may be required of smaller merchants, too.

EUROPEAN UNION

Council Regulation (EC) 792/2002, temporarily amending Regulation (EEC) 218/92 on administrative co-operation in the field of indirect taxation (VAT), introduces the additional measures necessary for the registering of foreign e-service traders for VAT purposes and for distributing the VAT receipts to the Member States where the services were actually used.

113 http://www.europa.eu.int/comm/taxation_customs/taxation/ecommerce/vat_en.htm

Under these new rules, EU suppliers are no longer obliged to levy VAT when selling in markets outside the EU, thereby removing a significant competitive handicap. (Under tax rules drawn up before e-service existed, EU suppliers had to charge VAT when supplying digital products even in countries outside the EU).

The changes eliminate an existing competitive distortion by subjecting non-EU suppliers to the same VAT rules as EU suppliers when they are providing electronic services to EU customers.

The VAT rules for non-EU suppliers selling to business customers in the Union (at least 90% of this market) remain unchanged, with the VAT paid by the importing company under self-assessment arrangements.

Direct e-commerce transactions (for example, the download of software, films, or music etc.) are subject to substantially different treatment under the VAT Directive[114] since they qualify as the supply of services. Whether or not VAT is due under the VAT Directive will depend on the place where the supply is deemed to be made.

A supply of services is deemed to be made in the EU Member State in which the supplier either (i) has a fixed establishment from which the supply is made; or (ii) is resident or usually resides. There are, however, a number of exceptions to this general rule, the most significant of which provide that:

- with regard to cultural, artistic and scientific, education, entertainment or similar services, the supply is deemed to be made where the service is physically carried out; and
- with regard to the supply of services (which includes the transfer or assignment of intellectual property rights, the supply of advertising services and the supply of information and data processing services) the supply is deemed to be made either in the EU Member State where the supply is received or the EU Member State in which the Vendor belongs.

In particular, if the Buyer resides within the EU and is a taxable person, the supply is deemed to be made in the EU Member State in which the Buyer resides and the Buyer is required to account for the VAT under the reverse charge procedure. Further, if the Buyer resides within the EU but is not a taxable person, the supply is deemed to be made in the EU Member State where the Vendor belongs and the Vendor is required to collect and account for the VAT. Finally, if the Buyer resides outside the EU, the supply is deemed to be made outside the EU, and VAT should not be charged.

European countries typically apply a VAT to foreign purchases through customs. In addition, the VAT is collected at each stage of production. Even if it is not collected at the final stage, it will have been collected at earlier stages.

114 Council Directive 2002/38/EC

Nonetheless, Europe has expanded efforts to tax e-commerce. For example, in June 2000, the European Commission proposed that downloaded digital products be classified as services, rather than goods. Normally, this would mean they would be taxed at the country of origin. Therefore, downloads from abroad would not be taxed. The final legislation was passed in February 2002, and took effect in July 2003. It required foreign companies pay the tax rate of the country of their consumers, but digital goods are just a small fraction of on-line purchases.

These measures mean that the EU became the first significant tax jurisdiction in the world to develop and implement a simplified framework for consumption taxes on e-services in accordance with the principles agreed within the framework of the Organization for Economic Co-operation and Development (OECD)[115]. The Directive therefore complements the international process at the OECD. The OECD principles on the taxation of e-commerce were agreed at a 1998 conference in Ottawa. These principles establish that the rules for consumption taxes (such as VAT) should result in taxation in the jurisdiction where consumption takes place. The OECD also agreed that a simplified online registration scheme, as now adopted by the Council, is the only viable option today for applying taxes to e-commerce sales by non-resident traders.

The Loopholes

The problems presented by electronic commerce for the integrity of VAT are not in themselves new; it is more a question of electronic commerce exacerbating existing tensions and difficulties inherent in the tax when dealing with cross-border transactions, relating particularly to place of supply and enforcement issues for non-resident suppliers of services. In finding solutions, the principle of any VAT system, of taxing the final consumer in the jurisdiction where the particular goods or services have been consumed and enjoyed, will have to be taken into account. An equally important principle is that goods and services that are provided across borders are zero-rated by the supplier in the country of origin. This is to ensure that consumers in the recipient country do not carry the burden of a foreign tax.

The question is whether existing indirect tax principles can be successfully applied to the taxation of electronic commerce in a way that will satisfy the competing demands of national revenue collecting agencies.

Similar to the sales tax, the VAT does not easily resolve the unique challenges such as definitions of physical presence, record keeping and standard categorization of transactions. The VAT hinges[116] on the geographic location of consumption. In e-commerce, it is difficult to locate taxable transactions outside the territorial scope of the common VAT systems. In

115 www.oecd.org.

116 www.ksg.harvard.edu/project1/vat.html

addition, the retention of the records of electronic commerce complicates the administration of the VAT. An on-line calculation where a web-based company sells multiple products to multiple countries with multiple customers becomes extremely difficult to track. Since the VAT is calculated and collected at the time of the transaction, it becomes near impossible to correct these errors once a sale is completed.

Now that businesses can more easily move to more tax-friendly jurisdictions, and can in some cases change their sources of income by using the Internet, most governments are concerned about the potential loss of tax on major revenue sources. The question is how to define a business establishment for ecommerce purposes. Multinational insurance companies, for instance, that cannot recoup their VAT, have to pay tax on the software that they buy. The easiest approach is to pay the tax in the country of their headquarters. The challenge here is how to prevent companies from opening offices in low tax jurisdictions where they have little or no business, simply to declare their taxes there. Already, it seems clear that business-to-business (B2B) transactions continue to develop, thanks to the ability of companies to forge new relationships globally through co-operative procurement designed to reduce costs and inventory.

The Suggested Solution

The global demand for an appropriate international framework for the taxation of electronic commerce that also reduces the risk of double taxation suggests that trading partners should participate in a common reevaluation of VAT rules, policies and administrative procedures. The design of a global tax framework is a matter of concern to all nations. Electronic commerce helps to expose differences in national tax systems. A global and comprehensive tax framework may be needed to correct those differences. In order to produce increasing convergence in the national tax regimes dealing with electronic commerce, the global market forces may require a comprehensive global tax framework. To succeed, a global framework requires international participation and cooperation, but in first place we need to bring the domestic regulations to a common point, binding contractual parties by the same financial obligations related to sales and taxes. Consequent violations through fraud must be punished accordingly with fines and imprisonment.

DISPUTE RESOLUTION

The Problem

The European Commission opened the door to alternative dispute resolution mechanisms. Alternative dispute resolution (ADR) solutions are developed to solve the disputes arising on the network, thus contributing to answer to consumer expectations. ADR is seen as a complement to judicial

procedures, its aim being to propose a tailor-made solution better adapted to the particularities of the network than is available in traditional court procedures[117]. As a matter of fact, ADR is currently the best solution to resolve disputes arising between a consumer and a service provider on the Internet. The reason for this is easy to understand: out of court dispute settlement should be particularly useful for some disputes on the Internet because of their low transactional value and the size of the parties, who might otherwise be deterred from using legal procedures because of their cost.

Be it through negotiation, conciliation, mediation or arbitration, ADR represents an attractive solution and has numerous advantages: (a) its flexibility allows an adapted procedure and an adapted solution, within a limited period of time and at low cost value; (b) its confidential nature is also of importance for businesses that might prefer to see their conflicts solved without any publicity; (c) an alternative solution presents fewer difficulties with regard to the enforcement of the decision, compared to the difficult enforcement of a judicial decision, especially in an international environment.

ADR solutions should however not develop outside a strict framework where minimal requirements are complied with, notably:

- the information of the consumer: a first range of information should include all the necessary information enabling the consumer to understand the purpose of the mechanism and its way of functioning; a second range should focus on the voluntary character of ADR that does not prevent the parties from going to court at any stage of the alternative procedure;
- the explicit consent of both parties to submit the dispute to the third party, before and/or after the dispute arises. Furthermore, consumer associations should be invited to play an active role in the setting up of ADR rules and procedures;
- the neutrality of the third party asked either to impose a solution or to advise the parties involved in the dispute;
- the compliance with the legal requirements regarding consumer protection.

The uncertainty about the way disputes arising on the Internet are resolved implies that the potential of e-commerce still to be exploited. The development of alternative solutions will undoubtedly help in the development of electronic commerce.

The Existing Texts

Consumers need to know that if something goes wrong with a transaction, there are effective ways of handling complaints and getting redress. Going to court to enforce your rights can be costly and time consuming, particularly if

117 Norman Solovay and Cynthia Reed - The Internet and Dispute Resolution: Untangling the Web- 2003

the trader is in another country. Good Codes of Practice and Alternative Dispute Resolution (ADR) schemes can often offer a range of remedies that can be less costly and less daunting.

The codes of practice can help to protect consumer rights and can offer consumer protection and service above the basics set down in law. They can improve consumer confidence and help businesses, because they can be easily modified in order to keep pace with rapid market developments.

Some governments believe that self-regulation by means of an effective code of practice can be a viable alternative to regulation. This is because legislation can be inflexible and difficult to change. Regulation can also impose unnecessary bureaucracy and additional costs upon business that can have an adverse effect on consumers through increased prices.

The Organization for Economic Cooperation and Development worked on a policy for Codes of Practice and Alternative Dispute Resolution (ADR) schemes (such as ombudsmen and arbitration). Both offer low cost and friendly alternatives to going to court.

The provisions of Private International Law are also relevant to cross-border transactions and disputes. The 1968 Brussels Convention, which deals with jurisdiction in cross border civil and commercial disputes, was replaced by a Community Regulation in December 2000. The 1980 Rome Convention already deals with which country's law applies in contractual disputes. In January 2003 the European Commission presented a Green Paper on the question of whether the Convention should be converted into a Community Instrument (a Regulation or Directive). A proposal was expected in 2005.

In July 2003, the European Commission presented a proposal for a Regulation on the law applicable to non-contractual situations, known as Rome II. The Regulation affects the treatment of claims involving defamation, advertising, intellectual property rights, and product liability.

In November 2003 the Council approved EU accession to Council of Europe Convention 180, the first truly international system open to more than 50 countries, including the US, Japan and Canada, of regulatory dialogue on information society services. The main focus was to strengthen international co-operation, to develop international rules on subjects such as the liability of Internet intermediaries (who provide access to the Internet and the transmission and hosting of information), procedures for removing illegal content, electronic contracts and out of court dispute resolution.

In a statement following the 2002 US-European Union Summit in Washington, the United States and the EU reaffirmed their support for the development of measures to boost consumer confidence in electronic commerce (e-commerce) and alternative dispute resolution. Both of them wanted to generate consumer confidence, but ensuring consumer protection and generating consumer confidence requires a combination of private sector initiatives and a clear, consistent and predictable legal framework. They agreed

that if parties cannot resolve consumer issues directly, the use of ADR is one means of doing so. Easy access to fair and effective ADR, especially if provided online, has the potential to increase consumer confidence in cross-border electronic commerce and may reduce the need for legal action.

In order to promote consumer confidence, ADR mechanisms should however be fair[118] and effective. There are general principles to achieve fairness and effectiveness: the impartiality of any decision-makers; the accessibility of the systems and procedures, which should be easy to find and easy to use; the need to ensure that the mechanisms are at low or no cost to the consumer relative to the amount in dispute; the transparency, including the importance of providing consumers with clear and conspicuous information about the procedures and commitments involved sufficient to enable informed choice and decision-making; and the timeliness of redress. At the same time stakeholders should continue to work to implement these fundamental principles in the context of particular ADR mechanisms, taking into account the value, the complexity and other characteristics of the transaction or dispute at issue.

The Loopholes

The possible negative impacts of ADR systems might include:

- Lack of consumer choice: Vendors may attempt to require consumers to use ADR mechanisms, whether they wish to or not
- Binding arbitration: If one or both parties are bound by the decision, their ability to seek legal redress if they are not satisfied may be restricted or blocked altogether.
- Intervention by others: If complaints are not brought to legal authorities or enforcers of codes of conduct, they may be unaware of problems that merit their attention. Moreover, ADR that is binding on consumers may prevent their cases from being used by legal authorities, code enforcers or others representing consumers' interests in broader actions to stop fraud or abuse.
- Disparity between the parties: Differences in language, cultures, and expertise in specific subjects may make it difficult for the parties to understand each other, and may lead to unfair results. Furthermore, if ADR systems lack adequate independence, the parties may not be treated equitably and decisions may be biased.
- Costs: If costs are assessed to support the operation of ADR systems, they may be prohibitively high for consumers or small businesses.

118 www.useu.be/TransAtlantic/US-EU%20Summits/ Dec1800USEUSummitWashington.html

- Enforcement: If parties fail to comply with decisions and there is no practical means of enforcement, the ADR process may be an exercise in futility.

The Suggested Solution

In light of the above the suggested solution for dispute resolution should be based on the following principles which are not exhaustive:

- The necessary framework and standards for ADR systems should be set by legislation.
- ADR systems should be easily accessible and convenient. Businesses which participate in such systems should provide links from their websites. Governments, consumer organizations, trade associations and others should also provide links to make it easy for consumers to find help. Disputes and responses should be able to be made online as well as offline. Real time discussions should be scheduled at the convenience of the parties. Physical or technical barriers to the ease of use for either party should be avoided.
- Information about the types of disputes handled, the procedures, the costs, the languages that can be accommodated, the basis for decisions (codes of conduct, etc.), the enforceability of decisions, and other details should be provided prominently and clearly.
  ADR systems should be designed and presented as a voluntary option for consumers, not as a legal or contractual requirement
- ADR systems should be free or low-cost. If the consumer is obliged to pay a fee for this service, the other party should refund the cost if the consumer prevails.
- ADR systems should be independent. They should be operated by reputable third parties, which could include government, nonprofit organizations, for-profit entities that are not directly involved in the disputes, or any combination thereof. If ADR systems are offered by trade associations or other industry groups, they should be separate and independent, and operate in consultation with consumer organizations. ADR personnel should have no direct interests in the disputes or the parties involved. If funding for ADR systems comes from the business sector, that commitment should be honored regardless of the decisions that are rendered.
- ADR personnel should be trained both in basic legal concepts and in mediation skills. If it is a collegiate body that will consider the dispute, equal representation should be given to consumers and businesses. If one single individual will consider the complaint, both disputants should be consulted in selecting that person, or the person should have been previously appointed by consumers and industry together.

- ADR systems should handle complaints in an expeditious manner. There should be reasonable time limits set for considering disputes, rendering decisions, and complying with decisions. If the parties are allowed to submit or ask to share documents or other evidence prior to the dispute being considered, there should be reasonable time limits set for that process.
- ADR systems should treat the parties equitably and fairly. While the parties should have the right to advice from legal counsel or others, the parties should represent themselves in the proceedings. If necessary, ADR systems should provide for translation or outside expertise.
- Decisions on behalf of consumers should be binding on the other party, except that appeals could be made on grounds of mathematical mistake or other technical problems. Meaningful enforcement of decisions rendered through ADR is essential. If ADR systems are operated by trade associations or other industry groups to which companies belong, compliance with ADR decisions should be a requirement for maintaining membership. Failure to comply with ADR decisions should also be a basis for those who facilitate the vendor's sales, such as online auction sites, operators of billing systems, etc. to deny future services to the seller. In addition, governments should adopt and, to the extent possible, harmonize legal frameworks to make ADR decisions enforceable. Consumers should have the choice of enforcing ADR decisions through the legal framework of either their or the vendors' countries.
- Consumers who submit disputes to ADR systems should not be asked to waive their legal rights, nor should they be restricted or blocked from resorting to other avenues of recourse that would normally be available if they are not satisfied with the outcome. Furthermore, consumer use of ADR systems should not prevent law enforcement authorities, code enforcers, or others representing consumer interests from using their cases in actions to stop fraud or abuse.
- In order to ensure that patterns of abuse do not escape the notice of legal authorities or relevant code enforcers, ADR systems should report all cases to a central clearinghouse from which that information would be accessible to the public.

Due to the special and complex issues raised by cross-border e-commerce disputes, further work will be necessary to develop specific guidelines for how ADR systems should be designed to provide the most efficient and effective redress for consumers.

CHAPTER 14. INTELLECTUAL PROPERTY

The Problem

Everything in cyber-space is composed of bits, the binary code that is the foundation of computing. In their digital form, images, music, video, and text are perfectly reproducible; not just once, but an infinite number of times. There is no degradation to limit the value of duplicate copies. With digital media, all copies are originals.

The binary reality of digital media poses vexing problems for how works are used and reused, as well as the rights and responsibilities of producers and consumers under existing law. One of the virtues of the Web is its reach: the ability to widely distribute digital works faster and less expensively than ever before. There is great value in being able to communicate to millions of people. The downside is that content owners have little control over the subsequent dissemination and use of their work. Too many consumers unaware or confused by expansive license agreements, or willing to dismiss them as overly restrictive or unfair, approach the Internet in the erroneous belief that every item that they encounter is in the public domain.

Intellectual property is a legal term that refers to industrial property and to copyright and related rights. Industrial property comprises the protection of patents, trademarks, industrial designs, and geographical indications[119]. It also includes the protection of utility models against unfair competition or the protection of undisclosed information. Trade secrets are protected, as they are a type of property or asset, just as valuable or even more valuable than physical or real property. The value of intellectual property assets relative to physical assets has increased because of the importance of technology and creative works in the modern economy. Intellectual property consists of new ideas, original expressions, distinctive names, and appearance that make products unique and valuable[120]. Intellectual property is often traded (or licensed) in its own right without trading in the value of an underlying product or service, by means of patent or other intellectual property licenses from a rights owner to another.

The character of the intellectual property system is evolutionary and while the nature of the rights themselves remains relatively constant, the manner by which they are expressed and exchanged is constantly adapting to developments in the underlying technologies. The invention of, in turn, the printing press, phonograms, radio and television broadcasting, cable and satellite transmission, videocassette recorders, compact disc (CD) and digital versatile disc (DVD) technology and now, the Internet, has affected both the form and the substance of intellectual property rights. Intellectual property has gained importance in this digital environment as, increasingly, business assets

119 http://www.1000ventures.com/business_guide/ipr/geo_indications_main.html
120 www.wipo.org/sme/en/e_commerce/ip_ecommerce.htm

are reflected in intellectual as opposed to physical property. The value of many online companies, for example, may be found in their vast databases of customer information, which may be the subject of intellectual property protection.

This migration of intellectual property onto the Internet can be seen with respect to each species of rights[121]. In the field of copyright, vast numbers of works of literature, film and art, and notably computer programs, have already been transferred to the digital environment. Software, protected as a form of intellectual property by patent and copyright law, underlies the operation of all digital technologies. Systems software, including utilities and operating systems, enable our computers to operate, while utilities software provides us with the programs that make the digital networks so useful. Much software is protected by intellectual property law, and yet its theft is endemic.

The copyright is created automatically when a qualifying work is created but it protects only the work itself and not the idea behind the work. This means that the copyright is only infringed by copying. So, if your competitor uses the ideas behind your successful e-commerce website to develop a very similar website independently, then it will not necessarily be infringing your copyright by doing so.

Textual works such as books and newspapers are ideally suited to digitization and, although online publishing of popular literature has had a mixed reception with a public accustomed to paper and ink, there is evidence of a growing demand for e-books. There has been real success in the online availability of science, technology and medical publications, where the demand for fee-based research has supported the e-publishing industry. Demand has also grown for the online collections of more than 7,300 libraries that have provided free remote access to the texts of hundreds of thousands of e-books.

In the field of fine art, indigenous craft and artifacts, numerous museums and art galleries have digitized their collections and made them available for viewing on the Internet.

Identity on the Internet also goes beyond the trademark system, because of the role played by the Internet domain name system, which facilitates the ability of users to navigate the network. Domain names are user-friendly addresses that correspond to the unique Internet Protocol numbers that connect our computers to the Internet and enable the network routing system to direct data requests to the correct addressee. Domain names were originally intended to perform a purely technical function in a user-friendly way, but because they are intuitive and easy to remember they now perform a function as business or personal identifiers. Most businesses, whether e-commercial or not, advertise their domain name to signal a Web presence. In this way, although, as such, not a form of intellectual property, domain names now

121 http://www.ecominfo.Internet/arts/878_shepherd.htm

perform an identifying functions similar to that of a trademark. Because of the way in which people and search engines operate, most businesses use their trademark or trade name as their domain name, and this has caused conflict with the advent of predatory practices.

The patent system has also migrated to the Internet, as businesses have sought to recoup research and development costs in digital technologies by patenting their online business methods. In fact, the technology-intensive nature of e-commerce means that many of its constituent processes may be patentable subject matter so long as the legal criteria for patentability are met.

The global information society foreseen in the early days of the Internet has yet to become a worldwide reality, but the focus on information remains the key to the e-commerce economy. Although a good proportion of the information on the Web is in the public domain, and freely available to use and copy, an increasingly significant amount is protected as intellectual property. The enthusiasm generated by the availability of so much online information, easily accessible through browsing and hyper linking, contributed to a general expectation that this information was free and its use uncontrolled. The intellectual property community has been addressing the challenge of this perception ever since[122], in an effort to determine and exert legal rights over digital content.

The intellectual property community, including film and music creators, software developers, authors and publishers, are now exploring ways in which to make their products available online, while protecting their rights and recouping their investment. To some extent, the uptake of fee-based intellectual property services is dependent on the efficient management of these rights, as well as the availability of workable and secure methods of micro payments that would enable pay-per-unit purchases, and the building of consumer confidence in online payment security, privacy and consumer protection. At the same time, however, creators and intellectual property rights holders need to feel sure that they can protect their property from piracy and control its use, before they will be willing to make it available online.

The online distribution of audiovisual works has been held back until recently by the lack of bandwidth, which has prevented the relatively large data files required to transmit video to be downloaded or streamed at a speed or quality acceptable to consumers. While the technology is still developing to facilitate accessible video-on-demand and digital pay-per-view, the film industry is yet to match the progress of the music industry, and most legitimate film sites are web casters that distribute short made-for-online film and animation material which is largely experimental and available free of charge. As in the music industry, copyright owners in the film industry are also reluctant to

122 http://www.1000ventures.com/business_guide/ipr/e-commerce_main_bywipo.html

release their audiovisual works online while there is a lack of adequate copy protection that could protect them from rampant piracy.

In the radio and web casting industry, Internet radio has been luring customers away from traditional media sources by providing access to thousands of global radio broadcasts in real time.

The Existing Texts

Intellectual property law is confusing because of the number of multilateral conventions that have been concluded in an effort to harmonize national laws. Increasingly these conventions have had direct effects on national law. With the growth of trade, and now, with the Internet, it has become important to understand not only the law of one's own jurisdiction, but also the law of other jurisdictions and the international conventions that regulate intellectual property by means of bilateral and multilateral commitments. Here are just few examples[123]:

EUROPEAN UNION

The European Parliament and the Council of the European Union adopted Directive 2001/29/EC on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society in May 2001. This Directive serves, to implement a number of the new international obligations provided under the World Copyright Treaty (WCT) and the World Performances and Phonograms Treaty (WPPT) [124]. The European Community's instruments of ratification will be deposited with World Iintellectual Property Organisation (WIPO) following the deadline for the Member States to transpose the Directive into their national legislation. The Directive contains a number of important implementation provisions, including those concerning the application of the right of reproduction in the digital environment; the right of making interactive transmissions available on networks such as the Internet; limitations and exceptions in the digital environment; technological measures for protection; and rights to the management of information.

Title 4 and Article 10 of the Council of Europe's Convention on Cyber-crime is named *Offenses related to Infringements of Copyright and Related Rights*. Paragraph one cites the four documents which parties must align their current domestic law with, namely, the Paris Act of July 1971 and the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property, and the WIPO Copyright Treaty[125].

The Diplomatic Conference on Certain Copyright and Neighboring Rights Questions gives the right to authors and artists to make their works available to

123 http://www.cptech.org/ip/business/us#us

124 www.wipo.org/copyright/ en/activities/wct_wppt/wct_wppt.htm

125 http://ecommerce.wipo.int

the public, giving the right of *commercial rental to the public of the original or copies of their work*.

Article 4 of the Directive of the European Parliament and the Council on the harmonization of certain aspects of copyright and related rights in the information society gives authors or creators of intellectual material the right to have their work prohibited from the public by any means. The directive on the legal protection of databases states that in any database that is protected by copyright, the author will have the power to alter its contents in any way he/she sees fit, including reproducing in any form. Article 4 also states that the author of the database shall be *the natural person or natural persons who created the base.* Article 6 aligns itself with the provisions of the Berne Convention for the protection of Literary and Artistic Works.

Article 3 defines on what terms a database will be protected under a copyright. Here, any work which is the authors own doing will be protected, and this will be the only criteria used to apply such a copyright protection.

USA

The United States of America[126] enacted legislation entitled the WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998 as Title I of the Digital Millennium Copyright Act (DMCA). Title I of the DMCA contains, among other things, provisions to implement obligations concerning technological measures and the management of the rights. Title I of the DMCA also requires the United States Copyright Office to conduct two studies jointly with the National Telecommunications and Information Administration of the Department of Commerce, one dealing with encryption and the other with the effect of technological development on existing exceptions in the Copyright Act, as part of an ongoing evaluation on the relationship between technological changes and the copyright law. Accordingly, two reports have been submitted to the Congress. Title II of the DMCA entitled the *Online Copyright Infringement Liability Limitation Act* deals with the issue of the liability of service providers based on a copyright-specific approach.

CHINA

Chapter II Article 8 of China's Regulations on Computer Software Protection states that a *software copyright owner shall enjoy the following rights*: *authorship, alteration, reproduction, distribution, rental, communication, and translation.* Article 14 states that a copyright awarded *shall be the lifetime of the natural person.* Article 16 states that *owners of duplicate software items have the right to load those items into a computer, to make back up copies of those items, and to take steps to enhance their performance*. Articles 18, 19, 20, and 21 address Licensing of Computer Software Protection. Here, a contract must exist before another person can *exercise*

126 http://www.usembassy.it/file9909/alia/99091414.htm

software copyright. This contract must be in writing and its entry into effect must be authorized by the Copyright Administrative Department.

JAPAN

Japan's Trademark Law states its purpose as the following:, *"The purpose of this Law shall be to ensure the maintenance of the business reputation of persons using trademarks by protecting trademarks, and thereby to contribute to the development of industry and to protect the interests of consumers"*.

Chapter II addresses issues regarding trademark registration. Here, *any person may obtain a trademark registration of a trademark to be used in respect of goods or services in connection with his business*. Exceptions are laid out and they include trademarks which deceive costumers. Section 5 of the chapter lays out the necessary process of re-registering for a trademark. Chapter III makes way for an *examiner* to examine all applications for trademarks. An examiner may refuse a trademark on the basis that it did not comply with the rules of application or other pertinent parts of Chapter II. Chapter IV addresses the enforcement of a trademark. A registration fee is to be paid after the examiner has accepted the trademark. The trademark right shall be 10 years from the date of registration, but a renewal is allowed after that date. The owner of a trademark has the rights of exclusive use, which include the right to *use the registered trademark in respect of the designated goods or designated services to the extent laid down in the contract granting such right.* In addition, *a right of exclusive use may be transferred only with the consent of the owner of the trademark right*. The document also makes way for the right to use a trademark by virtue of prior use and the right to use a trademark after expiration of a patent right. Chapter IV outlines the process for opposing the issuing of a trademark. Chapter V deals with a trial that may ensue to question an examiner's decision to refuse the issuing of a trademark. Chapter VI outlines the process of retrial and litigation of issues pertaining to the preceding chapters. Chapter VII deals with the ability of the owner of a trademark right to *obtain a defensive mark registration of a mark identical with the registered trademark with respect to goods or services for which such possibility of confusion exists.* The chapter also deals with acts deemed to be an infringement. Here, acts of holding and assigning, including *acts of manufacturing or importing goods bearing a reproduction of the registered defensive mark*. Chapter VII addresses the international registration of trademarks. Anyone seeking international recognition of a trademark must file that request with the Commissioner of the Patent Office, and must specify the names of the states for which trademark protection is sought. Chapter VIII entitled *Miscellaneous Provisions* addresses false marketing. Finally, Chapter IX deals with penalties, including fraud and dual liability.

WIPO

The 1996 WIPO Treaties (the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty) require that Contracting Parties make available adequate legal protection and effective legal remedies to protect

technologies used by rights holders. An essential element of adequate protection and effective remedies is legal protection against devices that circumvent technological measures. It is therefore only natural that border measures be extended to cover devices the primary purpose of which is to defeat such technologies used by rights holders to protect their intellectual property.

The Loopholes

While the world is getting larger with its expanding cyber-space, the world intellectual property system is still at its infancy. Different countries or territories have different intellectual property rules, practices and procedures. Strategic e-intellectual property management has its defensive and proactive aspects. On the defensive side, one has to avoid infringing intellectual property rights. On the proactive side, one should manage its intellectual property by strategic acquisition, licensing and enforcement.

It is submitted that a key success factor in ecommerce is strategic e intellectual property management. Any member of the information society who loses sight or underestimates the impact of intellectual property on e-commerce may have to learn it the hard way, paying a high price for intellectual property infringement or lack of intellectual property protection.

The international exhaustion is not solely a legal issue; there are economic and political aspects which must be balanced[127]. Arrangements may exist where a number of countries decide to form a single regional market, in effect defining a single regional territory. In such an arrangement, a requirement for freedom of movement of goods within a single market may lead to the acceptance of the legitimacy of parallel imports between countries which are party to the arrangement, provided that those countries together agree among themselves that such a restriction of the rights of a patentee is necessary in the realization of such a single market.

The following states do not apply a rule of international exhaustion of patents: Australia, Belgium, Brazil, Bulgaria, Czech Republic, Denmark, Egypt, Finland, France, Germany, Hungary, Italy, Japan, Korea, Mexico, the Netherlands, Paraguay, Portugal, Republic of Korea, Romania, Spain, Sweden, the United Kingdom, United States and Yugoslavia. In contrast, Argentina, Canada, Singapore and Venezuela do apply a rule of international exhaustion of patents.

Countries including the Member States of the European Economic Area (EEA), Bulgaria, Czechoslovakia, Hungary, Romania, the US and Yugoslavia do not apply a rule of international exhaustion for trademarks. In contrast, Argentina, Australia, Brazil, Canada, Japan, Paraguay, Mexico, Singapore, Switzerland, Venezuela and Yugoslavia all allow international exhaustion.

127 lists.essential.org/pipermail/ hague-jur-commercial-law/2001-December/000385.html

There are obviously various approaches and a lack of uniformity in international exhaustion.

This question raises the distinction between the common law approach to exhaustion and the approaches of different countries. The common law approach is that a sale of goods is a contractual matter, and that treatment of Intellectual Propert Rights (IPR) may be affected by the contract. In other countries, the treatment of IPR cannot be limited by contract. In a majority of countries, exhaustion is considered to be a matter governed by the legal effect of IPR, which are property rights having effect against all third parties. It is thus not possible for a contract between individuals to have any effect on the position. This is the legal theory, for example, in Brazil, Czech Republic, Paraguay and Yugoslavia. In contrast, in Japan (for patents at least) international exhaustion may be limited by contract and where there is a breach of contract, no exhaustion takes place. The Japanese position for patents is that if a patent owner fails to impose a contractual restriction on sale outside Japan then, irrespective of whether there is a parallel patent in the country of sale, the patentee is deemed to have waived his rights to prevent importation into Japan. In contrast, for trade-marks, the law is not clear. In Australia contracts may be effective in the case of patents, but not in the case of trademarks. In Canada it is necessary to bring a contractual restriction to the attention of a purchaser if it is to be effective. In Singapore contractual restrictions cannot be imposed to limit the effect of international exhaustion. In Japan the law differs for patents and trademarks.

Inventions are characteristically protected by patents. Inventions must also be protected by other types of rights, such as utility models or trade secrets. The patent system provides a framework for innovation and technological development by, on the one hand, granting an exclusive right to the owner of a patent to prevent others from commercially exploiting the patented invention for a limited period and, on the other hand, balancing this right with a corresponding duty to disclose the information concerning the patented invention to the public. This information, which is stored in the patent documentation, is available to anyone and, is increasingly accessible online through Internet-based systems. The mandatory disclosure of the invention thus enriches the available pool of technological knowledge, facilitates technology transfer, and enhances the opportunities for creativity and innovation by others.

The patent system plays a vital role in e-commerce, and relies in a critical way on various computer and network technologies. However, the new technologies pose challenges to the conventional legal scheme for the patent system[128]. It is expected that the number of these e-commerce-type patents may increase significantly, bearing in mind the potential for individuals,

128 www.ip4all.ch/E/jurinfo/documents/j110403e.pdf

companies and national economies, as well as the global economy. Such patents are viewed by some as important for creating incentives and spurring investment in new digital technologies. But the subject matter of a patentable invention must have a technical character or involve technical teaching, (an instruction addressed to a person skilled in the art as to how to solve a particular technical problem using particular technical means).

Since the phenomena of digital networks and e-commerce are new and still emerging, the novelty of a business model in this area makes the requirements of patentability a tenuous task. That competition may be harmed in cyber-space if companies are able to obtain patents for basic business methods that already exist in non-cyber-space.

In addition to the question as to whether computer programs should be regarded as inventions under patent law, this broad scope of patentability has prompted a discussion of where the line is to be drawn between copyright and patent law protection for computer programs.

The Internet raises complex issues in jurisdictional and enforcement of rights, as patent protection is provided on a country-by-country basis, and the patent law of each country has application only within its borders, in accordance with the traditional principles of territoriality. For example, where patented software is sold and delivered over the Internet internationally, any infringement action would require a consideration of the jurisdictional and choice-of-law issues. The first practical issue may be that of detection, since the unauthorized importation of such software by means of the Internet, unlike the importation of tangible goods, cannot be detected and stopped by customs authorities.

In the area of patents, one specific question may arise with respect to the law applicable to infringements when a patented invention consists of elements that are physically located in different territories[129]. For example, in the case of process patents for a method to process and transfer certain data using computerized networks, distinct elements in the process could be performed in different territories. If an alleged infringer operates a system containing all of the claimed elements within the territory in which the invention is protected, there would be a straightforward claim for infringement. The question of applicable law (and jurisdiction) would be more difficult where a patented invention involves activities in several countries by several individuals.

Prior to the development of the Internet as a medium for commercial exchanges, consumers rarely entered into direct relationships with foreign vendors. Typically, foreign products were distributed through local importers from whom consumers residing in the territory would make purchases. As a result of the global presence that the Internet enables, this model will no longer apply in many instances. Consumers can place orders on, or performs

129 www.wipo.org/copyright/ ecommerce/en/ip_survey/chap4.html

downloads from, the sites of foreign vendors, thus entering into a direct contractual relationship with them. This shift in the business model has important legal reverberations from the consumer protection point of view. As consumer protection is regarded a matter of public policy in many countries, these questions have proven particularly vexing to solve.

The Suggested Solution

The fundamental difficulty in coping with legal relationships involving foreign elements flows from the fact that the legal systems of more than one country may be involved. The application of the laws of one system, rather than that of the other, will lead to different results. One solution to this problem consists of selecting the laws of one particular legal system to govern the legal relationship, from among the various potentially applicable legal systems.

A radically different solution consists of trying to remove the source of the problem, through a process of harmonization which eliminates the differences that exist between the laws of countries on a given issue. Harmonization can be achieved through negotiations between states, with treaties establishing uniform rules under a universal code and the subsequent modification of domestic laws in order to bring them in line with the treaty provisions.

CHAPTER 15. OBSCENE PUBLICATIONS

The Problem

The Internet has given rise to a new industry for the online publication and consumption of obscene materials. Millions of people around the world are visiting web-sites catering to this product. These Internet sites represent the largest growth sector of the digital economy.

An obscene publication is generally understood to be any publication whose dominant characteristic is the undue exploitation of sex, or of sex together with crime, horror, cruelty or violence. Whether a publication's dominant theme is the undue exploitation of sex is determined by reference to a "community standards" test. Obscene article contains an image or a description of sexual behavior which is, arguably, an exceptional practice or a minority taste, or something which is beyond the pale and carry the risk that viewers of the material may be encouraged or corrupted into such practices.

A work is indecent if it, taken as a whole, appeals to the prurient interest in nudity, sex, or excretion; depicts, represents or describes in patently offensive ways, ultimate sexual acts, normal or perverted, actual or simulated sadomasochistic acts or abuse; or lewd exhibition of the genitals, pubic area, buttocks, or post-pubertal female breasts[130].

Obscenity is calculated to promote the violation of the law and the general corruption of morals[131]. The exhibition of an obscene picture is an indictable offence in law, if it be averred that the picture was exhibited to sundry persons for money.

However, for something to be obscene it must be shown that the average person, applying contemporary community standards and viewing the material as a whole, would find:

- that the work appeals predominantly to prurient interest;
- that it depicts sexual conduct in a patently offensive way; and
- that it lacks serious literary, artistic, political or scientific value.

An appeal to prurient interest is an appeal to a morbid, degrading and unhealthy interest in sex, as distinguished from a mere candid interest in sex. The first test to be applied, therefore, in determining whether the given material is obscene, is whether the predominant theme or purpose of the material, when viewed as a whole and not part by part, and when considered in relation to the intended and probable recipients, is an appeal to the prurient interest of the average person of the community as a whole, or the prurient interest of members of a deviant sexual group, as the case might be.

The predominant theme or purpose of the material, when viewed as a whole, means the main or principal thrust of the material when assessed in its

130 www.protectkids.com/dangers/pornlegaldefinitions
131 www.lectlaw.com/def2/o002.htm

entirety and on the basis of its total effect, and not on the basis of incidental themes or isolated passages or sequences.

The Existing Texts

For most countries[132] the current legislation relating to pornography has adapted itself to the Internet. Countries appear to be ready to co-ordinate their efforts to arrest the offenders and to share information readily with other countries, perhaps more so with child pornography than any other offensive material. This may of course be due to the fact that the majority of countries have ruled child pornography as illegal, even if levels of tolerance differ enormously.

AUSTRALIA

The Australian Broadcasting Authority (ABA) published a comprehensive report into the regulation of online services in Australia in 1996. This ABA report is perhaps the most comprehensive analysis of its kind available today.

The Department of Communications and the Arts (DCA) and the Commonwealth Attorney-General have jointly released a consultation paper, proposing the introduction of criminal offence provisions relating to the publication of objectionable materials.

Offences include the publication of objectionable material on an online service and for the publication of material unsuitable for minors in a way that makes it accessible to minors. Defenses include compliance with a code of practice and taking reasonable steps to avoid committing an offence, or holding a reasonable belief that the material published or made accessible was not objectionable, or in respect of material unsuitable for minors, that the material was not unsuitable for minors, or that the recipients would be or were in fact adults.

AUSTRIA

In March 1997, a Viennese ISP had all its computer equipment seized by police in connection with securing evidence against a child pornographer. At present, there appear to be no clear definitions of the position of ISPs or the extent of their responsibility for content. This has led to the establishment of the Austrian Internet Service Providers Association which plans to create an Internet Coordination Office to accept warnings of illegal content and cooperate with the authorities to coordinate these issues among the ISPs.

CANADA

As early as the summer 1993, a man was arrested, charged, and convicted for distributing obscene pictures and child pornography with his personal computer. In September 1995, the Canadian Information Highway Advisory Council (IHAC) tabled a series of recommendations mainly in the areas of information controls in hate literature and pornography, privacy and copyright.

132 http://www.ilpf.org/groups/content/toc

It also recommended the harmonization of information control legislation to deal with the question of the liability of users, owners, operators, the overall emphasis of this approach is on public awareness and industry self-regulation. The Canadian government's Department of Industry has commissioned a study of Internet content liability issues in order to establish who may be liable under present laws for online libel, copyright violations, obscenity and defamation.

CHINA

In February 1996, China's State Council adopted a draft law regulating the Internet, requiring all existing computer networks to liquidate and re-register all Internet providers, and to route these through the Ministry of Ports and Telecommunications. The rules forbid the production, retrieval and spreading of pornographic or obscene material or information which may hinder public order. Any institutional or individual service provider failing to route through the Ministry of Posts and Telecommunications and failing to register with the relevant authorities could be warned, suspended and fined by the public security department. A fortnight later, more rules were announced, requiring all Internet users to register with the police and to sign an agreement promising not to harm the country or do anything illegal. Individuals and institutions are required to register the fact that they are connected to the Internet with the local police within 30 days or face an unspecified punishment.

FRANCE

In May 1996, French Internet providers blocked access to 7,000 newsgroups for a week as a protest against the action under which two ISPs, FranceInternet and WorldInternet, had been raided for carrying pornographic images of young children. The two managing directors were also arrested and charged with disseminating pornographic pictures of minors. The obligation of access providers to offer technology to their customers to filter content has remained since then. This is the only regulation in existence for access providers in France. France has also been campaigning internationally for the Internet to be considered as a broadcasting medium, and therefore to be regulated by broadcasting law.

GERMANY

In December 1995, CompuServe cut off access to 200 news groups after Bavarian State prosecutors notified the US-based company that it was investigating distributors of sexually explicit material on the Internet. State prosecutors had advised CompuServe that it could face charges. Since CompuServe had no technology which could block access to a specific geographical location, access had to be blocked worldwide and the newsgroups were suspended for almost 5 million users worldwide. This led to accusations of censorship. In February 1996, CompuServe reinstated all but five news groups and planned to offer a parental control program so that users would restrict access to questionable sites. Edzard Schmidt-Jotzig, the German Justice

Minister, announced in June 1996 that new regulations for the Internet were to be introduced at the end of the year and the law was under consideration in Germany's lower house of parliament. The law is now known as the *Federal Law regulating the Conditions for Information and Communication Services*, and was approved in the cabirnet in December 1996.

INDIA

India has one government-owned Internet service provider, VSNL, which has approximately 14,000 subscribers. VSNL has ruled out censorship of web-sites including those containing pornographic material, with its Director of Operations stating that, *Total censorship on sites that host material that is revolting to our culture is not viable.*

INDONESIA

In December 1996, the House of Representatives passed a broadcasting bill into law. It primarily affects television stations but also seeks to regulate new forms of broadcasting, including teletext, audiotext and the Internet. It outlaws violence, sadism, pornography, mysticism, a permissive lifestyle, consumerism, hedonism and feudalism. As is apparent from this list, the definitions are vague, and need more explanation to be enforceable. Although anyone broadcasting through these new media is required to obtain operating licenses from the government, the law appears to be more relaxed about content, stressing self-censorship by the operators. The clause dealing with the Internet is vague and needs clarification.

SINGAPORE

Under the powers conferred by Section 18 of the Singapore Broadcasting Authority Act, the Singapore Broadcasting Authority (SBA) issued the Internet Code of Practice, with effect from July 1996. Under these guidelines, all Internet Service Providers and Internet Content Providers must use their best efforts to ensure that nothing is included on the Internet that offends good taste or decency, in particular content which is pornographic or otherwise obscene, content which depicts or propagates gross exploitation of violence, nudity, sex or horror or content which depicts or propagates sexual perversions such as homosexuality, lesbianism and pedophilia

UNITED KINGDOM

The Obscene Publications Acts of 1959 and 1964 make it an offence to publish obscene material. These Acts define publication to include distribution and circulation of obscene material. Publishers of obscene article, including distributors, have a defense if they have not examined the material and had no reasonable cause to suspect that the nature of the articles was such that these publications would make them liable to be convicted of an offence[133]. It applies to online services.

133 http://www.jisc.ac.uk/uploaded_documents/lis_cyber-crime.pdf

USA

The US Telecommunications Act of 1996 includes various provisions intended to combat obscene and indecent communications. Part of the Act provided that, among other things, any person who, "*by means of a telecommunications device knowingly ... makes, creates or solicits* and *initiates the transmission* of *any comment, request, suggestion, proposal, image or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, shall be criminally fined or imprisoned*".

EUROPE

Convention on Cyber-crime,

Article 9 – Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another;

e. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4. Each Party may reserve the right not to apply, in whole or in part, paragraph 1(d) and 1(e), and 2(b) and 2(c).

The Loopholes

Very little information is available about the Internet porn industry. Many online pornographers operate under an ineffective regulatory regime that permits virtual anonymity. Accordingly, it is difficult to ascertain the extent and popularity of the Internet porn business. What is known is that pornography is comprised of legal as well as illegal elements. Many national governments are focused on preventing the production, distribution and consumption of pornographic materials involving children. State resources are being committed to the Herculean task of monitoring and surfing the Internet for child porn. Government efforts to combat child pornography involve interaction with

various aspects of the adult Internet porn sector, much of which is legal in several states.

The anonymous and paperless nature of the Internet serves as an incentive for the electronic transmission and purchase of pornographic goods and services. Government authorities encounter difficulties because the whole process of marketing, distribution, payment and delivery of obscenities can be completed electronically without the need for physical delivery or legal identification of either the consumer or the e-commerce vendor. The intangible nature of Internet porn eliminates the paper trail that is a fundamental component of criminal investigations and international tax audit and verification practices[134].

The popularity of the unregulated Internet is now causing difficulties. Porn sites are notorious for their annoying pop-up and pop-under advertising windows. Huge amounts of unsolicited e-mail are widely sent with much of it attributable to adult web sites. The proliferation of offensive materials is deterring the use of the Internet as an educational tool for youth. Recent studies indicate that children continue to be regularly exposed to lawful, sexually explicit materials on the Internet. Internet pornography detracts from the social and economic benefits of e-commerce, and national governments are being driven to regulate the Internet to control these harmful practices.

Many governments around the world have been slow in extending the application of their criminal laws to address the proliferation of illegal porn and obscene materials on the Internet. Enforcement difficulties abound because Internet markets are global while criminal laws differ from country to country. Nonetheless, national governments and international police have increased the amount of economic resources dedicated to the monitoring of the Internet and the enforcement of child pornography laws.

Due to the lure of huge profits and the lack of effective criminal sanctions, pornographers are expending economic resources to promote the production and consumption of Internet porn. The inequity of this economic shift of resources becomes more pronounced when consumers forego purchasing from local outlets in favor of shopping online to avoid paying sales and other transaction taxes. National governments should take immediate steps to remove the tax loopholes exploited by porn vendors and consumers.

The Suggested Solution

If the illegal and harmful content on the Internet needs to be regulated then the question is: how should this be achieved? Despite the popular perception, the Internet is not a lawless place. The Internet is a complex, anarchic, and multi-national environment where old concepts of regulation, reliant as they are upon tangibility in time and space, may not be easily

134 www.innovationlaw.org/ pages/taxingobsceneprofits.2004.doc

applicable or enforceable. This is why a wider concept of governance may be more suitable.

There appears to be no single solution to the regulation of illegal and harmful content on the Internet because the exact definition of offences related to obscene publications and what is considered harmful varies from one country to another. What is obscene in one country may be highly protected speech in another. A recent European Commission Communication Paper stated that each country may reach its own conclusion in defining the borderline between what is permissible and not permissible. A multi-layered governance system should be a mixture of national and international legislation, and self-imposed regulation by the ISPs and on-line users. This should include codes of conduct by the ISPs, software filters to be used by parents, advice to parents and school teachers, hotlines and special organizations to report illegal content on the Internet. But the base of the pyramid must be the universal legal framework that needs to criminalize the publication, distribution and selling of obscene materials over the Internet and to prosecute them accordingly. Needless to say, without full international cooperation, the implementation of the above recommendation on a global level would be totally ineffective.

CHAPTER 16. DIGITAL SIGNATURES

The Problem

A digital signature is a form of electronic signature. The term electronic signature is used to describe the full range of electronic means in order to confirm the sender of the message. These range from a file including a graphical image of the sender's handwritten signature (simple but unreliable) to biometric techniques such as iris scans (complex but reliable).

The digital signature is a digital code that can be attached to an electronically transmitted message that uniquely identifies the sender. Like a written signature, the purpose of a digital signature is to guarantee that the individual sending the message really is who he or she claims to be.

Digital signatures are based on public key technology, a special form of encryption invented in the 1970s which uses two different keys[135]. As two different keys are used, this form of encryption is also known as asymmetric cryptography. One key is kept secret (the private key) whereas the other key is made publicly available (the public key). The two keys are generated simultaneously and they are collectively known as a key pair. Once a message has been encrypted using one of the two keys, it can only be decrypted by the other key.

When sending a message over an open network such as the Internet, public key cryptography can ensure confidentiality of the message. The public key cryptography can also be used to verify the identity of the sender and the integrity of the message.

Digital signatures are especially important for electronic commerce and are a key component of most authentication schemes. To be effective, digital signatures must be unforgeable. There are a number of different encryption techniques to guarantee this level of security. A signature is not part of the substance of a transaction, but rather of its representation or form. Signing writings serve the following general purposes:

- Evidence: A signature authenticates writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.
- Ceremony: The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent inconsiderate engagements.
- Approval: In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it has legal effect.
- Efficiency and logistics: A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen

135 www.bakernet.com/ecommerce/ Digital%20Signatures-Addressing%20the%20Legal%20Issues.doc

> the subsequent need to inquire beyond the face of a document. Negotiable instruments, for example, rely upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.

To achieve the basic purposes of signatures outlined above, a signature must have the following attributes[136]:

- Signer authentication: A signature should indicate who signed a document, message or record, and should be difficult for another person to produce without due authorization.
- Document authentication: A signature should identify what is signed, making it impracticable to falsify or alter either the signed matter or the signature without detection.

Signer authentication and document authentication are tools used to exclude impersonators and forgers and are essential ingredients of what is often called a nonrepudiation service in the terminology of the information security profession. A nonrepudiation service provides assurance of the origin or delivery of data in order to protect the sender against false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent. Thus, a nonrepudiation service provides evidence to prevent a person from unilaterally modifying or terminating legal obligations arising out of a transaction effected by computer-based means.

Digital signatures identify and authenticate the originator of the information. They allow the receiver to ascertain the identity of the sender and to determine and verify whether the message has changed during transit.

The core concern of electronic signature legislation has been electronic documents, sometimes referred to as records or electronic records, and signatures that are created, communicated, and stored in electronic form. Generally, these signatures are referred to as either electronic signatures or digital signatures. Unfortunately, these terms themselves have created considerable confusion[137]:

Electronic signature is a generic, technology-neutral term that refers to all of the various methods by which one can sign an electronic record. Although all electronic signatures are represented digitally (i.e., as a series of ones and zeroes), they can take many forms and can be created by many different technologies. Examples of electronic signatures include: a name typed at the end of an e-mail message by the sender; a digitized image of a handwritten signature that is attached to an electronic document; a secret code or PIN (such as that used with ATM cards and credit cards) to identify the sender to the recipient; a code or handle that the sender of a message uses to identify

136 http://www.univie.ac.at/RI/AJLI/3/menzel/menzel1.htm

137 www.bakerInternet.com/ecommerce

himself; a unique biometrics-based identifier, such as a fingerprint or a retinal scan; and a digital signature (created through the use of public key cryptography).

Digital signature is simply a term for one technology-specific type of electronic signature. It involves the use of public key cryptography to sign a message, and is perhaps the one type of electronic signature that has generated the most business and technical efforts, as well as legislative responses.

A signature, whether electronic or on paper, is first and foremost a symbol that signifies intent. The primary focus, of course, is on the intention to authenticate, which distinguishes a signature from an autograph. Yet, the nature of that intent will vary with the transaction, and in most cases can be determined only by looking at the context in which the signature was made. A signature may, for example, signify an intent to be bound to the terms of the contract, the approval of a subordinate's request for the funding of a project, the confirmation that a signer has read and reviewed the contents of a memo, an indication that the signer was the author of a document, or merely that the contents of a document have been shown to the signer and that he or she has had an opportunity to review them.

In addition to evidencing a person's intent, a signature can also serve two secondary purposes. First, a signature may be used to identify the person signing. Second, a signature may serve as some evidence of the integrity of a document, such as when parties sign a lengthy contract on the final page and also initial all preceding pages to guard against alterations in the integrity of the document through a substitution of pages.

For electronic transactions, these secondary signature functions of identity and integrity can be the key. To the extent that electronic transactions are automated, and conduct them over significant distances using easily altered digital technology, the need for a way to ensure the identity of the sender and the integrity of the document becomes pivotal: Unlike the world of paper-based commerce, where the requirement of a signed writing most frequently serves the function of showing that an already identified person made a particular promise, in the e-commerce world, a requirement of an authenticated electronic message serves not only this function, but the more fundamental function of identifying the person making the promise contained in the message in the first place. This additional function is critical in e-commerce because there are few other methods of establishing the source of an electronic message.

Thus, while handwritten signatures in most cases serve merely to indicate the signer's intent, signatures in an electronic environment typically serve three critical purposes[138] for the parties engaged in an e-commerce transaction, (a) to identify the sender, (b) to indicate the sender's intent (for example, to be

138 www.usaid.gov/locations/ europe_eurasia/pdfs/armeniaictpub.pdf

bound by the terms of a contract), and (c) to ensure the integrity of the document signed.

The Existing Texts

A wide range of actors are involved in digital signature issues: different departments and agencies of national governments, individual corporations, industry associations, civil society organizations, inter-governmental organizations at the regional and global levels, and other international groups and organizations, some of which are multi-partite while others may represent a single stakeholder group.

At regional level, both the OECD and APEC have done a lot of work on e-commerce and maintain working groups that meet regularly to advance their work programs. The focus of these organizations has been on analyzing issues related to e-commerce, diffusing information, and developing guidelines and recommendations intended to help coordinate national policies and practices among their members. Although they are inter-governmental organizations, they have involved other actors in their work.

At the international, inter-governmental level:

The World Trade Organization (WTO) helped lay the foundation for e commerce through its agreements on trade in telecommunications and other services, and is the source of the moratorium agreement not to impose customs duties on e-commerce. The WTO has also maintained a work program on e-commerce for a number of years. Rather than involving negotiation of a specific international agreement on e-commerce, this program has provided a horizontal forum for identifying and examining the implications of e-commerce for the different types of trade dealt with by the WTO (trade in goods, services and intellectual property). This programme includes a capacity building component designed to assist developing countries;

The United Nations Conference on Trade and Development (UNCTAD) and the associated International Trade Centre (ITC) have done a lot of work identifying and analyzing e-commerce issues, particularly from the perspective of developing countries, and have important capacity-building roles;

The World Intellectual Property Organisation (WIPO) has concluded two Internet treaties that update international copyright law so that it applies to digital works, and maintains an ongoing Digital Agenda to address issues related to e-commerce. In addition, WIPO provides the Domain Name Dispute Resolution Service that arbitrates disputes about IPRs in domain names[139];

The United Nations Conference on International Trade-Related Laws (UNCITRAL) has developed a model e-commerce law that has been adapted and applied in a number of countries;

139 www.wgig.org/docs/WP-Ecommerce.pdf

The United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) develops recommendations aimed at facilitating trade through the electronic exchange of trade-related information between government agencies and the private businesses;

The International Telecommunication Union (ITU) has developed technical standards related to e-commerce and has a technical assistance program that aims at building capacity in relation to the technical and business underpinnings of e-commerce.

While participation in the formal governance activities of inter-governmental organizations is generally limited to governments, the ITU is a notable exception in that it a wide variety of non-governmental actors in all but its treaty-making activities. However, all intergovernmental organizations generally incorporate non-governmental actors in their informal activities in advisory or consultative roles, including those related to e-commerce, in advisory or consultative roles.

Other international fora that have been active in e-commerce include:

- Long-established business organizations, such as the International Chamber of Commerce which has maintained a very active work programme that produces reports and recommendations for its members, national governments and international organizations on a wide range of issues related to e-commerce;
- Special initiatives by the business community, such as the Global Business Dialogue, which does policy research and advocates on e commerce issues;
- Multi-partite initiatives, such as the G8 DOT Force and the UN ICT Task Force, which have included representatives of national governments, the private sector, civil society and international organizations, and which have addressed selected issues related to e commerce.

Yet a quick look at the electronic signature legislation currently enacted or under consideration reveals that while there is agreement on where we ultimately want to go, there is little agreement on how to get there. Legislation ranges from a minimalist approach[140] that simply authorizes the use of electronic signatures in very limited circumstances, to legislation that establishes some evidentiary presumptions and default provisions that parties can contract out of, to a very formal and highly regulatory approach governing the manner in which digital signatures may be used and certification authorities may operate.

Most legal systems have reduced formal requirements, or at least have minimized the consequences of failure to satisfy formal requirements. Nevertheless, this process is still in the beginning and various legal barriers still

140 www.ilpf.org/groups/analysis_IEDSII.htm

exist. Any case relating to electronic commerce is characterized by the absence of written documents and their substitution with electronic documents. To avoid difficult procedural requirements for daily used transactions which are only electronically recorded several proposals demand a more or less equalization of the legal effects between hand-written and digital signatures. The formal requirements for legal transactions, including the need for signatures, vary in the different proposals.

EUROPEAN UNION

The EU Directive on a Community Framework for Electronic Signatures 1999/93/EC, dated 13 December 1999, (Electronic Signatures Directive) lays out the general framework for the use of electronic signatures for reliable and legally valid communication by electronic means.

Article 2 (1) of the Electronic Signatures Directive defines simple electronic signatures as *data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication*.

Further, Article 2 (2) of the Electronic Signatures Directive defines advanced electronic signatures as electronic signatures being:

i) uniquely linked to the signatory;

ii) capable of identifying the signatory;

iii) created using means that the signatory can maintain under his sole control; and

iv) linked to the data to which it relates in a manner that any subsequent changes to the data are detectable.

Advanced electronic signatures require authentication by a Certification Services provider, operating in accordance with the principles set out in the Electronic Signatures Directive. Each advanced electronic signature is materially identified by a specific qualified certificate containing various characteristics prescribed in Annex I of the Electronic Signatures Directive. These include, in particular, the designation as an advanced electronic signature, the identification of the Certification Services provider, the duration of the certificate and any other inherent limitations as to the scope and value of transactions covered by the certificate.

Article 5 (1) of the Electronic Signatures Directive stipulates that only advanced electronic signatures which have the same legal effect as hand-written signatures in the individual EU Member States, are admissible as evidence in legal proceedings. With regard to simple electronic signatures, Article 5 (2) of the Electronic Signatures Directive provides that EU Member States must ensure that such signatures are not denied legal effect or admissibility as evidence in legal proceedings solely on the grounds that they do not qualify as advanced electronic signatures. In consequence, when effecting Business to Business (B2B) or B2C e-commerce transactions, a vendor must evaluate the general accessibility of advanced electronic signatures, as opposed to simple electronic signatures, for buyers.

USA

The US electronic signature law (Electronic Signature in Global and National Commerce Act of 2000) eliminates legal barriers to using electronic technology to sign contracts, to collect and store documents, and to send and receive notices and disclosures. Under the Act, no contract, signature or record can be denied legal effect solely because it is in electronic form.

In the E-Sign Act Section 106(5), the term electronic signature is defined broadly as follows: *"The term electronic signature means an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record".*

CANADA

In May 2004, the Canadian government took important steps regarding the use of digital signatures in Canada. Secure Electronic Signatures Regulations were first issued pursuant to the Canadian Personal Information Protection and Electronic Documents Act and the Canada Evidence Act. Later, Principles for Electronic Authentication were published by Industry Canada. These regulations and the principles facilitate the use of digital signatures in communications with the federal government and in electronic commerce.

ASIA

Legislation passed in Asia regarding digital signatures include Australia's Electronic Transactions Act 1999, South Korea's Electronic Transaction Basic Act; Japan's Draft Bill Concerning Electronic Signatures and Certification Authorities and the Law Partially Amending the Trade Mark Law; Malaysia's Digital Signature Act 1997, the Philippines' Electronic Commerce Act; and India's Information Technology Act 2000.

The Loopholes

It is a common opinion that many attributes of traditional paper-based communications contribute to satisfying the legal requirements for signatures. A company's name and logo appearing on a purchase order, the letterhead at the top of a correspondence, or the hand-written signature at the end of the document are examples which reinforce authenticity, verification of identity, non-repudiation and other functions of the written form. These attributes are lost or weakened by the move into electronic messages.

With electronic communications there can be no traditional writing and hand-written signing. The Internet is a place where spoofing and faking a false identity can be realized very easily[141]. When it is paper based, the medium and the message are inherently bound together, and are transmitted together as one physical object. In electronic information flows the medium is absent until it is displayed on the screen or printed out. Therefore, evidence law perceives reasonable differences in the quality of proof provided by traditional paper-

141 http://www.cle.bc.ca/contributors/profiles.asp?UName=FREBR0

based messages and simple electronic messages not secured with digital signatures.

It is a logical consequence that an electronic system follows totally different underlying principles, technical methods and uses different attributes to provide the same functionality for the users. It is most important that a signature should indicate the person who signed a document, message or record, and it should be difficult for another person to produce it without authorization.

The most crucial point to satisfy this requirement by the use of digital signatures is the possibility to access a private key[142]. According to the nature of the underlying technique of asymmetric encryption, anyone who has access to the private key can digitally sign messages indistinguishable to the certified holder of the responding key pair. The recipient of the message only can verify the content of the certificate, but he cannot be sure as to who is really using the private key to encrypt that message he has received. Restricting access to the private key only for the authorized user is therefore the most critical task in the complete system. This is done by the process of authentication, which is executed to check the authorization of a user before granting access to a private key for encrypting the hash code of a message. Authentication means the service designed to verify the user's identity. Identification and authentication can be made by knowledge (for example: password protection), by possession (for example a smart card), or by checking the user's human characteristics (biometrics).

At a low security level the private key is stored on the hard disk of a computer, which is often connected to the network. Knowledge of a password is the only authentication to get access. The next step to secure private keys is to store them on a medium, which is physically in the exclusive possession of the certified key pair holder. Smart cards might comply with this condition, because the hardware of the card is designed to prevent the extraction of the data of the private key. These techniques satisfy the requirement of authentication as long as the smart card remains in the exclusive possession of the corresponding certificate holder.

Another possibility to prevent any voluntary undermining of authentication is to force the restriction of use only to the certified person with technical methods. Instead of authorizing the access privileges with a password check, the system could also verify the matching of biometric attributes of the user.

For e-commerce to develop and flourish, both consumers and businesses must be confident that their transaction will not be intercepted or modified, that the seller and the buyer are who they say they are, and that transaction

142 http://www.bakerinfo.com/ecommerce

mechanisms are available, legal, and secure. Building such trust and confidence is the prerequisite to win over businesses and consumers to e-commerce.

Trust, of course, plays a role in virtually all commercial transactions. Regardless of whether the deal is struck in cyber-space or in the more traditional paper-based world, transacting parties must trust the messages that form the basis for the bargain. Trusting a message, from a legal perspective, requires consideration of the authenticity and integrity of the message, as well as an assessment of whether the message is non-repudiable by the sender in the event of a dispute.

In many cases, the law requires agreements to be both documented in writing, and signed by the person who is to be held bound, in order for that agreement to be enforceable. Statutes and regulations that demand transactions to be in writing and signed are generally perceived to constitute barriers to e-commerce, which must be removed if e-commerce is to flourish.

Generally, a signature is any symbol executed or adopted by a party with present intention to authenticate a writing[143]. Thus, the key requirement is not the ink on paper, but rather the presence of a symbol coupled with the party's intention. Faxed signatures have also been assumed to constitute effective signatures. Thus, any symbol or code on an electronic record that is intended as a signature should also meet the requirement. Even a name typed at the end of an e-mail should qualify as a signature, so long as it was created with the proper intent.

Unfortunately, the legislative approaches to what appears to be a simple issue of merely removing barriers to e-commerce have been somewhat varied and inconsistent, and may have actually made the situation worse. In clarifying that electronic records meet writing requirements and that electronic signatures meet signature requirements, statutes have differed greatly regarding two fundamental issues: (1) what qualifies as a signature; and (2) what types of transactions can be undertaken using electronic records and electronic signatures.

Electronic signature legislation has also taken a variety of approaches regarding the types of transactions for which the use of electronic signatures is authorized. Nearly half of the states in the world expressly authorize the use of electronic signatures for virtually all transactions. Other states have statutes that authorize the use of electronic signatures only for certain categories of transactions. Some states, however, condition the authorization to use electronic signatures on the type of party involved in the transaction. For example, some statutes authorize the use of electronic signatures only where both parties are government agencies, while other statutes require at least one of the parties to be a government entity. In yet other states, statutes authorize

143 profs.lp.findlaw.com/signatures/signature_4.html

the use of electronic signatures only for transactions involving a specific private entity, such as a financial institution.

Taking such varied approaches to what qualifies as an electronic signature, what types of transactions can be undertaken electronically, and what types of parties may use electronic signatures, may only make matters worse for e commerce. For example, one problem created by statutes that authorize the use of electronic signatures only for transactions involving certain types of parties, or only for certain types of transactions, is that it raises a concern that, by implication, any other use of electronic signatures is not authorized. By providing for the enforceability of electronic signatures in certain limited types of transactions, the legislature may have implicitly evidenced an intention to preclude the enforceability of electronic signatures in other types of transactions. When different states set different standards as to what attributes are required for an electronic signature before it will be considered enforceable, businesses face daunting practical difficulties in using electronic signatures for transactions nationwide.

The Suggested Solution

Although it seems proper to reject the imposition of undue restrictions on e-commerce, one must recognize that legislation can, if properly written, encourage rather than restrict, and promote rather than disable, the desirable public policy goal of global e-commerce. The promotion of electronic signature legislation must distinguish between, (a) regulatory legislation, which often dictates restrictive standards and conditions, and (b) enabling or facilitating legislation, which can be used to support freedom of contract and which can increase predictability and certainty in online transactions without inhibiting the development of new business. Limiting the legislative helping hand that is extended to e-commerce is not risk-free; benign neglect may well produce stagnation or at least slow down the development of online businesses.

Electronic signature legislation can and should serve as a vehicle for advancing e-commerce, but it will no doubt need to adapt the legislative approaches as new business models and technologies emerge. In order to avoid future damage, international law must bind the contractual parties by the same obligations and regulations related to digital signature worldwide. Consequent violations through deception, forgery, theft etc, must be criminalized and punished accordingly with fines and imprisonment. Such prosecution of the perpetrators would be impossible without effective international cooperation.

CHAPTER 17. CIVIL LIBERTIES

The Problem

The growth of the Internet has challenged the basic civil liberties of citizens around the world. The advent of super-fast computing, high-bandwidth Internet access, huge data warehouses, anonymous online speech, ubiquitous e-mail, and the advance of tools to track these communications have all tested basic assumptions about these liberties. The specter of terrorists using Internet technologies to carry out their gruesome work has prompted increasingly stringent laws and regulations which have an even greater impact on the balance between civil liberties and law enforcement.

It is necessary in the first place to make the distinction that civil liberties[144] refer to conceptual rights, and civil rights refer to legal rights. In other words, civil liberties are personal rights as spelled out in constitutions and other founding documents, such as the right to life, liberty, the pursuit of happiness, free speech, freedom of religion, freedom of assembly, etc. Civil rights, on the other hand, are the particulars of how those vague concepts are implemented in law. Under this definition, civil liberties do not change, except when a constitution is amended, but civil rights change regularly as new laws are made, or new interpretations are ruled upon.

The right to privacy[145] as it has been developed in these cases reflects the values of a 19th century liberal democracy whose primary concern was to protect the individual from inappropriate interference from the state. The nature of communications networks now makes it equally pressing to protect against potential invasion of personal autonomy by private interests or individuals.

To resolve these issues, one has to first ask whether the values of individual autonomy, cultural inclusiveness and knowledge-sharing will determine the environment of electronic communications, or whether the building of the information highway will be driven by the market needs of large vested interests.

Privacy is the ability of an individual or group to prevent information about themselves from becoming known to people other than those they choose to give the information to. Privacy is sometimes related to anonymity, although it is often most highly valued by people who are publicly known.

The right against unsanctioned intrusion of privacy by the government, corporations or individuals is part of the laws of many countries, and in some cases, of the constitutions themselves. Almost all countries have laws which in some way limit privacy, for example taxation normally requires passing on information about earnings. In some countries individual privacy may conflict

144 http://www.antipope.org/charlie/journo/civil-lib.html

145 Top Ten Threats to Civil Liberties in Cyber-Space By Ann Beeson

with freedom of speech laws and some laws may require public disclosure of information which would be considered private in other countries and cultures.

Privacy may be voluntarily sacrificed, normally in exchange for perceived benefits, but often with little benefit. It is one of the areas of security where trade-offs become very clear and apparent. For the collection of taxes it is in the interests of government and, probably, the rest of society, that an individual's earnings and income are known. On the other hand, that same information may be used to select the individual or his family as a good target for kidnapping. There is an obvious contradiction between these two interests.

Individuals may wish to keep their political viewpoints secret for a variety of reasons; political groupings may be able to commit violence either when successful (using the powers of the state) or when defeated (using their own militias for example). This may be used to punish those who disagree with these views. Many people have been tortured or killed for their political views by dictators, terrorist groups, and even forces linked to democratically elected politicians. The secret ballot, which is common in democratic elections worldwide, is designed to maintain political privacy to limit any discrimination against voters, and to avoid revenge attacks by those who were not elected.

Information concerning a person's health is generally kept confidential in the doctor/patient relationship. In most countries, the patient must grant access before anyone other than the staff of medical institutions may view the information. The reasons for keeping medical information private may include possible discrimination against people with a certain medical conditions.

Many companies attempt to obtain as much information about customers as possible, through loyalty cards and other kind of customer schemes. This data is immensely valued by other companies, which may pay large amounts of money for access to this information, for marketing purposes.

Governments in many countries are given powers to breach privacy[146]. This is often due to criminal investigations, where police are permitted to seize private property from a suspect's house. Telephone tapping, where all information being transmitted over a phone line is secretly monitored, is often permissible for Law Enforcement Agencies[147] although it sometimes requires permission from a court. This can then be used as evidence in trials where it is used to secure convictions against criminals.

There is little, if any, evidence on the level of public concern about privacy in developing countries; the issue does not figure with any importance in the policy agendas of these countries. The problems of security, the cost of living and unemployment are all given higher priority.

Freedom of speech is the liberty to freely say what one pleases, as well as the related liberty to hear what others have stated. Recently, it has been commonly understood as encompassing all types of expression, including the

146 On Liberty in Cyber-Space: Impact of the Internet on Human Rights by Ekaterina Drozdova with Seymour Goodman
147 http://www.clas.ufl.edu/users/jakest/ch4_civil.htm

freedom to create and distribute movies, pictures, songs, dances, and all other forms of expressive communication.

Freedom of speech is often regarded as an integral concept in modern liberal democracies, where it is understood to outlaw government censorship. Free speech is also protected by international human rights law, notably under Article 19 of the Universal Declaration of Human Rights, although implementation remains lacking in many countries.

The right to freedom of expression is not considered unlimited; states may still punish certain damaging expressions of opinion. Restrictions on free speech are required to comply with a strict three part test: (a) they must be provided by law; (b) they must pursue an aim recognized as legitimate; and (c) they must be necessary or proportionate for the accomplishment of that aim. Amongst the aims considered legitimate are protection of the rights and reputations of others, and the protection of national security and public order, health and morals.

Information technology now makes it virtually impossible for governments and law enforcement agencies to control the exchange of information. Traditional approaches to regulating freedom of expression assume that the legal system is equipped to intervene. Courts can no longer be assured of their ability to enforce their decisions.

Encryption of communication has become a festering sore on the Internet civil liberties scene. It is virtually impossible to effectively ban all forms of encryption; and there are many reasons why a ban would be undesirable. Most Internet communications are carried out in plain text, but the need for encryption is increasingly necessitated by the requirements of safety for commercial transactions.

The freedom[148] of the press to print and distribute is explicitly guaranteed but is somewhat limited, particularly by laws governing obscenity and defamation. Telephone networks follow common-carrier principles, they do not impose content restrictions on the cargo they carry. It would be unthinkable for a telephone company to monitor calls routinely or to cut off conversations because the subject matter was deemed offensive.

Cyber-Space is probably the world's first true mass media because it allows anyone with a few simple tools to communicate ideas to thousands of persons at once. It inspires tolerance [149] and promotes mutual understanding by connecting people around the world. It is a tool for community organizing and citizen involvement. All this innovation and citizen empowerment inspired by online communications would be lost if your free speech and privacy rights do not apply in cyber-space.

148 Humanizing Cyber-Space: Privacy, Freedom of Speech, and the Information Highway by Professor Valerie Steeves
149 Herman Schwartz, Harvard College '53 Fiftieth Reunion Symposium , The Future of Civil Liberties June 4, 2003,

The Existing Texts

The European Convention on Human Rights, to which most European countries, including all of the European Union, belong, lists a number of civil liberties.

While the United Kingdom has no formal written constitution, it is a signatory to the European Convention on Human Rights which covers both human rights and civil liberties, and has passed the Human Rights Act, which forces compliance between the treaty and UK law. After the September 2001 attacks in the US, the UK claimed a state of emergency (as permitted by Article 15) and the derogation from Article Five in order to allow the indefinite detention without trial of foreign nationals suspected of involvement with terrorism. The government would rather deport these individuals, but this is prohibited by Article 3, which cannot be opted out from according to Article 15.

Despite the UK's liberal heritage, the Government's Information Commissioner stated in 2004 that the country is currently in danger of becoming a surveillance society.

The United States Constitution, especially its Bill of Rights, protects many civil liberties.

The Constitution of Canada includes the Canadian Charter of Rights and Freedoms which guarantees many of the same rights as the US constitution.

PRIVACY LAWS

Article 12 of the Universal Declaration of Human Rights states: *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks"*.

Most countries have laws protecting people's privacy. In some countries this is part of their constitution, such as the United States Bill of Rights, and France's Declaration of the Rights of Man and of the Citizen. If the privacy of an individual is breached, the individual may bring a lawsuit asking for monetary damages.

To date, government policies have created an uneven patchwork of rules designed to protect privacy. The Federal Privacy Act of 1982 of USA is based on the *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Information* adopted by the Organization for Economic Co-operation and Development (OECD) in 1980, which includes the following principles:

- *When data is collected, the purpose for the collection must be disclosed.*
- *The data collected must be relevant to the purpose for which it is collected.*
- *The data must reflect standards of quality and accuracy.*
- *Security safeguards must be established to prevent unauthorized access to the data.*
- *The data must only be used for the purpose for which it was collected, unless the consent of the individual has been obtained.*

- *The collector of the data must establish open policies regarding the nature of the data and the manner of its storage.*
- *The individual must have knowledge of and access to the data.*
- *The collector of the data must be accountable for its collection and use of the data*

PRIVACY AND DATA PROTECTION

Privacy concerns not only the context of law enforcement, but also day-to-day business practices and an individual's ability to control the treatment of personal data made available in electronic format or accumulated during Internet use. The commercial exploitation of personal data without consent is already leading to enhanced legal protections for privacy. The enforcement of such protections will raise the issue of the desirability of using protective versus reactive methods, leading to discussions of what can be done to ensure that any method used will protect privacy interests against unwanted intrusion.

Privacy is not an absolute, well-defined, or uniformly protected value[150]. Individuals, organizations, and societies have traditionally sacrificed some privacy in exchange for greater security, economic gain, or convenience. Trade-offs between privacy and intrusion reflect the different historical and social contexts in which they were made.

Protection of privacy has evolved historically through international and domestic law. Privacy is a fundamental human right recognized by the 1948 Universal Declaration of Human Rights and many other international and regional instruments and treaties. The Universal Declaration proclaims that *"no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation,* and *everyone has the right to the protection of the law against such interference or attacks.* It also states that *everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers"*. These provisions create the basic international law framework for the right to privacy, which extends to cyber-space.

On the national level, privacy is protected through a combination of constitutional and legislative instruments and self-regulation. Nearly every country in the world recognizes a constitutional right to privacy, including at least the rights to inviolability of home and secrecy of communications. Some recently written constitutions, such as those of South Africa and Hungary, contain rights to access and control of one's personal information. In countries where the right to privacy is not explicitly guaranteed by the constitution -the United States, Ireland, and India, for example- this right has been established through other legal provisions or judicial rulings. In the United States, for example, a strong privacy interest derives from the constitutional guarantees of security of person, house, property, and papers; protection against unlawful

150 www-hoover.stanford.edu/publications/ books/fulltext/cyber-crime/183.pdf

and unreasonable searches and seizures; the right against self-incrimination; and the freedom of speech and assembly.

The Organization for Economic Cooperation and Development (OECD) was the first international organization to issue a policy document, namely, *Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*, adopted in 1980. The OECD's policy applies to personal data, whether in the public or private sectors, that pose a danger to privacy and individual liberties because of their nature or the manner in which they are processed and used.

Development of international standards continued in the 1980s and 1990s. The Council of Europe (COE) adopted a *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data* (1981) and *Guidelines on the Use of Computerized Personal Data Flow* (1989). The United Nations (UN) produced *Guidelines for the Regulation of Computerized Personal Data Files* (1989). These documents establish principles of minimum privacy guarantees for personal information at all stages of its collection, storage, and dissemination by other parties. They also create new rights for data subjects (those whose data are collected and manipulated by government agencies, businesses, etc.) requiring that accurate and up-to-date personal information must be obtained fairly and lawfully; used only for the original, intended purpose; and destroyed after the purpose is achieved. Data subjects are granted the right to access and to amend information about them.

The 1995 European Union (EU) Data Protection Directive established a regulatory framework for the free movement of personal data, while allowing individual EU countries to exercise their unique approaches to implementation. Data subjects are guaranteed the right to know where the data originated, the right to have inaccurate data corrected, the right of appeal in the case of unlawful processing, and the right to deny permission to use data under certain circumstances.

The 1999 Council of Europe Recommendation provides guidelines for the protection of privacy on the Internet. While the COE and UN guidelines are recommendations, the EU directives are binding, as member states must adopt them into their domestic law.

FREE SPEECH

In democratic countries, the freedom of speech is taken for granted, though the exact degree of freedom varies between countries and jurisdictions. This freedom generally includes:

- the right to criticize the political system and political leaders, even those in power;
- the right to criticize public and corporate policies;
- the right to criticize religious and political ideas.

Still, freedom of speech is not absolute in any country. Limits include, for instance, the prohibition of libel and slander, and hate speech.

USA

In the United States, freedom of expression is protected by the First Amendment to the United States Constitution. There are many exceptions to this general rule, including copyright protection, the Miller test for obscenity, and greater regulation of so-called commercial speech, such as advertising.

Generally, the US has a liberal policy on freedom of expression, with no formal government censorship of the news media or creative arts. When expressive content is held to lie beyond the protection of the First Amendment, the finding is usually made by a court during a prosecution after the content is published or publicly exhibited. It might be argued that nevertheless the threat of post-facto punishment is sufficient to prevent certain types of speech from being uttered or broadcast in the first place.

ASIA

Several Asia countries guarantee freedoms of speech to their citizens. They are not however implemented in practice at most places. Some countries still repress freedom of speech, though with economic progress those barriers have been reducing.

The Indian constitution guarantees freedom of speech to every citizen and there have been landmark cases in the Indian Supreme Court that have affirmed the nation's policy of allowing free press and freedom of expression to every citizen.

EUROPE

The European Convention on Human Rights signed in November 1950, proclaimed a broad range of human rights already in existence in the signatory countries (the members of the Council of Europe). These rights include Article 10, which entitles all citizens to free expression. This right includes freedom to hold opinions and to receive and impart information and ideas without interference by public authority. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.

It also included some other restrictions: The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Each country then had to alter their laws to conform with these rights. In 1998, the United Kingdom implemented the Human Rights Act which granted the judiciary power to apply these rights to cases, and a requirement for Parliament to check the compatibility of new laws with the Convention. If a judge finds a law to be incompatible with the given rights, then the law must be amended to incorporate these protections.

Europe-wide cases have been heard in the European Court of Justice as well as in the European Court of Human Rights to guarantee these privileges.

FRANCE

Article 11 of the Declaration of the Rights of Man and of the Citizen states: "*The free communication of thoughts and of opinions is one of the most precious rights of man: any citizen thus may speak, write, print freely, save [if it is necessary] to respond to the abuse of this liberty, in the cases determined by the law*".

In addition, France adheres to the European Convention on Human Rights and accepts the jurisdiction of the European Court of Human Rights.

The right to criticize politicians and the government is cherished and taken for granted by the French population. France has a tradition of political lampooning and satirical writing. French law prohibits public speech or writings that incite to racial or religious hatred. In December 2004, a controversial addition was made to the law, criminalizing the prohibition to hatred or violence against people because of their sexual orientation.

France does not implement any preliminary government censorship for written publications; plaintiffs have to demonstrate the violation of law in court. However, press publications must have an identifiable director of publishing, and publications directed towards the youth have supplemental obligations. Also, the government has a commission recommending movie classification, the decisions of which can be appealed before the courts. Finally, the government restricts the right of broadcasting to authorized radio and television channels under authorizations which are granted by an independent administrative authority.

GERMANY

Freedom of speech is guaranteed by Article 5 of the German Grundgesetz. There are, however, some restrictions, for example personal insults or hate speech (Volksverhetzung). The latter includes the propagation of neo-nazi ideas and the use of nazi symbols like the swastika, except for purposes of art, research or education.

CANADA

The constitutional provision that guarantees Freedom of expression in Canada is section 2(b) of the Canadian Charter of Rights and Freedoms.

2. Everyone has the following fundamental freedoms: ... (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication.

Due to Section 1 of the Charter, the so-called limitation clause, Canada's freedom of expression differs from the provision guaranteeing freedom of speech in the United States of America in a fundamental manner. The section 1 of the Charter states:

The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it "*only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society*."

This section is double edged. First it implies that a limitation on freedom of speech prescribed in law can be permitted if it can be justified as being a reasonable limit in a free and democratic society. Conversely, it implies that a restriction can be invalidated if it cannot be shown to be a reasonable limit in a free and democratic society. The former case has been used to uphold limits on legislation which are used to prevent hate speech and obscenity.

In April 2004, Bill C-250 was passed which includes propaganda against people based on their sexual orientation as hate speech. It is now illegal to publicly incite hatred against people based on their color, race, religion, ethnic origin, and sexual orientation. However, under Section 319 on hate speech, a person cannot be convicted of hate speech *if the person can establish that the statements made are true.*

IRELAND

Freedom of speech is protected by Article 40.6.1 of the Irish constitution. However the Article qualifies this right, providing that it may not be used to undermine public order or morality or the authority of the State. Furthermore, the constitution explicitly requires that the publication of blasphemous, seditious, or indecent matter to be a criminal offence. Under the European Convention On Human Rights Act, 2003, all of the rights afforded by the European Convention form an integral part of the Republic of Ireland's laws. The act is, however, subordinate to the constitution.

AUSTRALIA

Unlike most other nations that legally protect freedom of speech, Australia does not have a bill or declaration of rights. However, in 1992 the High Court of Australia judged in the case of Australian Capital Television et al. v. Commonwealth of Australia (Adban) that the Australian Constitution, by providing for a system of representative and responsible government, implied the protection of political communication as an essential element of that system. This freedom of political communication is not a broad freedom of speech as in other countries, but merely a freedom which protects political free speech. It is also a shield, rather than a sword - as it does not establish a cause of action by itself.

AFRICA

The majority of African constitutions provide legal protection for freedom of speech. However, these rights are exercised inconsistently in practice.

The Loopholes

No speech should be subject to prior restraint or criminal prosecution unless it is intended to incite and is likely to cause imminent lawless action. Free speech[151] does not mean one can damage a reputation or appropriate a copyrighted work without being called to account for it. And it does not mean

151 Privacy In Cyber-Space By Pavan Duggal

that one can release a virus across the network in order to send a message to network subscribers. Although the distinction is trickier than it may first appear, the release of a destructive program, such as a virus, may be better analyzed as an act rather than as speech.

The law enforcement agencies and civil libertarians[152] must agree about the need to establish procedures for searches and seizures of particular computer data and hardware. They also will have to be trained to make use of software tools that allow searches for particular files or particular information within files on even the most capacious hard disk or optical storage device.

Developing and implementing a civil liberties agenda for computer networks will require increasing participation by technically trained people.

A policy on electronic crime should offer protection for security and privacy on both individual and institutional systems. Defining a measure of damages and setting proportional punishment will require further good faith deliberations by the community involved.

Network systems should be designed not only to provide technical solutions to security problems but also to allow system operators to use them without breaching unduly on the rights of users. A security system that depends on extensive monitoring of traffic, for example, would create more problems than it would solve.

Those parts of a system where damage would do the greatest harm, financial records, electronic mail, military data, etc. should be obviously protected. This involves installing more effective computer security measures, but it also means redefining the legal interpretations of computer crime and privacy so that system users are protected against individual criminals and abuses by large institutions. These policies should balance the need for civil liberties against the need for a secure, orderly, protected electronic society.

Privacy is threatened[153] by businesses and other entities that collect and manipulate personal data, criminals who steal such data or stalk people over the Internet, and governments that pursue surveillance or allow intrusive law-enforcement practices. Sophisticated electronic capabilities to collect, analyze, manipulate, and disseminate information, as well as to enable tracking, surveillance, and interference with communications, create unprecedented challenges to privacy.

Such technologies are becoming more effective, available, and affordable internationally. At the same time, globalization and growing dependence on information technology in all spheres of society have led to a dramatic increase in the level of electronically compiled and transmitted personal data. The differences in domestic legal standards and practices also endanger private data transmitted over international networks. Even if one state has robust privacy laws, it cannot currently guarantee equivalent levels of protection once the data

152 Crime-Facilitating Speech Eugene Volokh

153 www.ciaonet.org/wps/dre01/DrozdovaCivilLibert2000.pdf

flow beyond its borders. Gaps in protection will be created to the extent that laws and law enforcement fail to keep up with technological capabilities and international discrepancies undermine domestic levels of protection.

The Suggested Solution

Given the past record of many governments as intruders into such fundamental rights, the role of national governments as the defenders of privacy and of fundamental rights also needs careful consideration. Whilst society needs to be shielded from clearly antisocial conduct, there are strong arguments for permitting, and protecting, the anonymity of most web-site visits, and chat rooms where people can communicate with each other without fear that their interests, attitudes, beliefs and concerns will be monitored either by the public or the private sectors.

Governments must balance the need to protect public security with the need to protect individual rights to privacy. This balance becomes especially challenging when criminals are using digital technologies to plan and commit crimes.

The current environment of terrorist threats makes it tempting to shift this balance towards national security, and to encroach upon civil liberties beyond the previous balance point. Digital technologies can be used very effectively for information gathering and surveillance in many ways. In formulating laws and regulations with respect to cyber-space, cyber-crime, and critical infrastructure protection, it is important to use the new powers of digital technologies to gather information and access in a manner that continues to respect individual rights.

Given the technological change and the enhanced capacity of the Internet, there is an urgent need, for a review of information privacy principles. There are now serious gaps in those principles and some new privacy principles are needed, for example:

- The right to encrypt personal communications effectively;
- The right to fair treatment in public key infrastructures, so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy. The right to human checking of adverse automated decisions and a right to understand such decisions.
- The right of disclosure of the collections to which others will have access and which affect the projection of the profile of the individual concerned.
- The visibility of data collection practices. Any feature which results in the collection of personally identifiable information should be made known prior to operation and the individual should retain the ability to disengage the feature if he or she so chooses.

CHAPTER 18. CIVIL LIABILITY

The Problem

The principles of civil liability are codified in the laws of each state. Some of them are governed by Common Law, and others by Civil Law systems. The difference between Civil Law and Common Law lies less in the mere fact of codification, and more in the approach to codes and statutes. In Civil Law countries, legislation is seen as the primary source of law; by default, courts base their judgments on the provisions of codes and statutes, from which solutions in particular cases are to be derived. In Common Law systems, n the other hand, cases are the primary source of law and are used to induce the principles which should be applied in the situation to be resolved; statutes are only seen as incursions into common law and are thus interpreted narrowly. This explains the great importance of court decisions in the Common Law systems. Despite these differences in approach and methods, both systems usually lead to fairly similar decisions.

In general, civil liability law concerns situations[154] in which harm is suffered by a person due to an activity. The law then determines the situations in which there is liability, who is to assume the liability, and the way in which the prejudice is to be compensated. The principal situations which can generate damages and civil responsibility are those which cause:

- harm to reputation (defamation);
- invasion of privacy ;
- violation of secrecy;
- unfair competition.

In each of these situations, liability is not automatic and is not necessarily assigned to the access provider. An Internet service provider (ISP) is a business or organization that offers users access to the Internet and related services. Most telecommunications operators are ISPs. They provide services such as Internet transit, domain name registration and hosting, dial-up access, and leased line access. Liability does not depend on what one is, but rather on what one does or does not do when transmitting information. Generally, it is only after careful examination of the specific facts of each case that it can be determined whether there was any clumsy or negligent action taken by one of the participants in the production and transmission of a message which proved to be harmful.

Liability[155] on the ground of defamation is the publication of a false statement injurious to the reputation of another. Statements as used in the laws on defamation have been defined widely to include words, visual images,

154 http://ssrn.com/abstract= 605964
155 http://www.sudhirlaw.com/cyberlaw-itact.htm

gestures, and any other method of signifying meaning. The plaintiff only needs to prove:

- that there is a false statement about him/her;
- that the statement is published;
- that this was done intentionally or with reckless disregard for the truth; and
- that it causes damage to his/her reputation.

In English and American law, and systems based on them, libel is a form of defamation which is the tort or delict of making a false statement of fact that injures someone's reputation. Defamation is however the generally-used term internationally. In many legal systems, factual statements must be false to be defamatory. Proving statements to be true is often the best defense against a prosecution for libel. Statements of opinion which cannot be proven true or false will likely need to apply some other kind of defense. In some systems, however, truth alone is not a defense. It is also necessary in these cases to show that there is a well founded public interest in the specific information being widely known, and this may be the case even for public figures.

Defamation is of particular significance in publications made via the Internet. The Internet comprises a worldwide web, so issues involving multi-state defamation arise, and it may not be clear which court has jurisdiction and which law applies.

The principles which have been developed for newspapers or televisions apply on the Internet. Information placed by a web-site provider for access over the Internet is sent by that person to others (potentially millions of others, simultaneously in many different jurisdictions. However, the Internet does provide unique factual circumstances in which multi-state defamation may be committed in that it has the ability of making information available simultaneously in every jurisdiction in the world. Civil liability[156] arises from publications likely to harm a person's reputation and penalties are monetary.

There are numerous opportunities for defamation on the Internet: many long-time users of bulletin boards and chat rooms see the Internet as a place where one can take on any identity and say almost anything. Examples include user messages sent to all members of a particular Internet group or posted on a web site, defamatory material contained in a database, posting on a bulletin board or in a chat session, or specific e-mail messages sent and forwarded to one or more recipients.

The principles[157] of civil responsibility as they are understood in Common Law and in Civil Law establish a strict relation between the degree of effective control over information and the liability of the various participants in the

156 http://law.richmond.edu/jolt/v8i3/article18.html
157 http://www.mala.bc.ca/~soules/media301/Internet_law.htm

communications[158]. The nature and degree of the liability of Internet access providers clearly follows from the degree of control they exercise or are supposed to exercise over harmful information. This impliess that when the specific circumstances of a case of broadcast of actionable information reveal that the access provider had some control over the incriminating information, that provider will be assigned a share of the liability. As a corollary, an access provider when warned of the existence of a content problem risks liability if no intervention takes place.

However, in the present state of the law, it remains difficult to distinguish the circumstances in which an access provider should act to prevent prejudice from those situations which do not present a sufficiently clear case to justify an intervention, particularly if the latter could result in severe censorship. Without having access to the viewpoints of all those involved, it is indeed very difficult to determine whether a specific content is actionable. The general rule adopted across many jurisdictions is that civil liability tends to arise when an ISP fails to remove offensive material, provided it has been brought to their attention following a complaint (for example, child pornography). The ISPs tend to tread fairly carefully and be responsive to requests for cooperation. The access provider thus finds itself in the uncomfortable position of being criticized at some point for having permitted a content harming a person to circulate, when it is really very poorly placed to intervene in order to suppress a content of which the harmful nature is often far from obvious. Moreover, the principle of freedom of expression, as it is understood in democratic societies, concords poorly with practices in which access providers would pass judgment on the potentially actionable or harmful nature of information passing through their facilities.

The present state of civil liability law[159] calls for access providers to adopt preventive policies in order to manage their responsibility in the manner which is most compatible with the Internet, and so as to minimize, for themselves as for others, the harm which could be caused by actionable information on the Internet.

The Existing Texts

Europe's harmonized system of procedural and substantive law has its roots in the unifying principles of the 1957 Rome Treaty. The European Union formed new legal institutions to carry out its objective of transcending national borders. All twenty-five Member States are represented on the European Council, which drafts legislation for Europe as a whole. This unified approach has allowed Europe to take the lead in formulating a harmonized legal regime for the information age. The European Commission is charged with developing a legal framework to advance free competition in the Single Market.

158 http://www.cyberlawsa.co.za/cyberlaw/cybertext/chapter12.htm
159 http://www.ceece.org/law.htm

The Commission has powers of initiative, implementation, management, and control, which allow it to formulate harmonized regulations. In the past decade, the Commission has approved Internet regulations such as the E-Commerce Directive, E-Signatures Directive, Distance Selling Directive, Data Protection Directive, Database Protection Directive, and the Copyright Directive.

Internet jurisdiction cases in Europe follow the Brussels Regulation's "bright-line" rules rather than the standards-driven US style "minimum contacts" approach. The Brussels Regulation governs jurisdiction in civil and commercial disputes between litigants and provides for the enforcement of judgments throughout the European Union. The Brussels Regulation applies throughout Europe, while the US approach has yet to be adopted or borrowed by any other legal system.

A judgment rendered in a European Union country may be enforceable outside of its borders. The European Court of Justice, for example, ruled that the Brussels Convention applied to a Canadian company in a contract action brought in a French court [160]. The new Brussels Regulation governing jurisdiction and judgments applies to all Brussels Convention signatories except Denmark, which has opted out of the new regulations. The Brussels Regulation sets forth the general rule that persons domiciled in a Contracting State shall, whatever their own nationality, be sued in the courts of that State of domicile. European consumers, unlike their American counterparts, have an absolute right to sue a seller or supplier if the latter pursues commercial or professional activities in the Member State of the consumer domicile.

Americans courts, in contrast, enforce choice-of-forum clauses that require the consumer to litigate in the seller's home court. In tort cases, the place where the harmful event occurred is where jurisdiction applies.

Any entity doing business on the Internet may thus be subject to divergent tort rules in distant forums. In December of 2002, the Australian High Court held that a businessman could sue Barron's and Dow Jones for libel in the state of Victoria based on evidence that several hundred people in that state accessed the Dow Jones Web site where the allegedly defamatory article was posted. In the Dow Jones case, the Australian Court reasoned that the place of uploading of materials onto the Internet might bear little or no relationship to the place where the communication was composed, edited, or had its major impact. This decision made Australia the only country that allows an action against a foreign defendant based solely on an Internet download in that country. The Dow Jones case ultimately settled for $440,000 and legal fees in November 2004.

160 europa.eu.int/eur-lex/en/ com/pdf/2003/com2003_0427en01.pdf

Cyber-space will not fulfill its promise if web sites continue to be subject to hundreds of conflicting procedural and substantive rules simply because the material can be accessed in every nation of the globe.

The European Commission has formulated a draft of the Rome II Convention concerning which laws should apply in cross-border tort disputes[161]. The Rome II Convention for torts, delicts, or non-contractual relations, proposes uniform rules for resolving conflicts of law in European cross-border disputes. The Commission seeks to harmonize conflict rules, which must be distinguished from the harmonization of substantive law. The Commission believes that it is more efficient to have one single set of conflict of law principles in order to reduce the cost of litigation and to boost the foreseeability of solutions and certainty as to the law.

The European Commission is divided over how Rome II interrelates with the already enacted eCommerce Directive. The latter determines jurisdiction on the principle of country of origin. The country of origin approach subjects a company to regulation only in the country where the information originated, irrespective of whether information is transmitted to other Member States. The country of origin rule means that a service provider or e-business need only comply with the rules and regulations in one Member State as opposed to tailoring content for all of the countries of the European Community.

As opposed to that, Article 3(1) of Rome II adopts as its basic rule the law of the place where the direct damage arises or is likely to arise. In most cases this corresponds to the law of the injured party's country of residence. In a typical Cyber-space transaction, the place of purchase may be purely fortuitous, and under certain circumstances may even be virtually impossible to establish. Internet publishers fear that the Rome II Convention, which applies to online defamation cases, could result in publications having to pay libel damages under the laws of 100 different countries if defamatory material is published over the Internet. The Rome II Convention fails to recognize the possibility of publishers in one country being subjected to the libel laws of others, causing particular problems for Internet providers.

Choice-of-Forum in Cyber-Space

E-businesses reduce their exposure to unfamiliar laws by requiring all users worldwide to submit to the company's own choice of legal forum. Nokia, for example, inserts a conflict of forum clause into its mass-market contracts, requiring users to submit to arbitration in Helsinki, Finland, where Nokia has its headquarters.

American companies frequently require users to waive their jury rights in favor of arbitration. For example, America Online requires all of its customers to litigate any disputes in Virginia: *"These Terms of Use shall be governed by and construed in accordance with the laws of the Commonwealth of Virginia, excluding its*

161 www.jhtl.org/V5N1/04_JHTL_Lambert_RustadKoenig.pdf

conflicts of law rules. One expressly agree that the exclusive jurisdiction for any claim or action arising out of or relating to these Terms of Use or your use of this site shall be filed only in the state or federal courts located in the Commonwealth of Virginia, and you further agree and submit to the exercise of personal jurisdiction of such courts for the purpose of litigating any such claim or action".

Similarly, MCI requires all users to arbitrate any dispute under the law of New York, while forbidding arbitrators from awarding consequential damages or punitive damages. The agreement also shortens the statute of limitations to a period of one year. The rules for enforcing choice-of-forum clauses in cross-border e-commerce disputes have yet to be formulated. The validity of e-commerce mass-market license agreements is due in part to the US Supreme Court's willingness to legitimate one-side forum selection clauses as decided in Carnival Cruise Lines, Inc. v Shute. In Carnival Cruise, a Washington resident who was injured on a cruise ship argued that a Florida forum selection clause contained in her ticket was unenforceable because of the expense and inconvenience of litigating in Florida. The Court rebuffed this argument, holding that the forum selection clause was reasonable and enforceable even though the litigants were physically and financially incapable of pursuing their claims in Florida. Most American courts extend the principles of Carnival Cruise into cyber-space.

Americans and Europeans have fundamentally different legal traditions that reflect their unique national histories. The common law approach of creating law around precedent is found only in the Anglo-American legal tradition. Despite the dominance of civil codes that are derived from Roman law in all of the continental European countries, there are many national differences. Sweden and Norway for example, have a well-established ombudsman tradition for resolving disputes, which is not found in France. The European Community is now seeking greater harmonization through the use of Directives, which are broad legal principles that require implementing legislation in each individual Member State.

Divergent Defamation Regimes

Defamation is a common law tort action when a false oral or written statement [162] has been made that lowers the plaintiff's reputation in the community. The Internet raises complex substantive legal conflicts as to what constitutes a defamatory statement and how reputation is to be measured for Internet transmissions. With hundreds of countries connected to the Internet, it is unclear as to whose community standards apply.

The English definition of defamation was a communication to a third person that tends to hold the plaintiff up to hatred, contempt, or ridicule or to cause him to be shunned or avoided. What would be considered to be defamatory in England may be protected expression in the United States. The

162 www.murdoch.edu.au/elaw/issues/v1n3/loundy13.html

controversial boxing promoter Don King, who resides in Florida, filed suit against Lennox Lewis, a world champion boxer, a promotions company, and a New York attorney based upon an allegedly defamatory Internet posting that charged King with being anti-semitic. King chose the United Kingdom to file suit even though the statements were posted on California-based web sites, because the UK's defamation laws are decidedly more pro-plaintiff. In the United States, this lawsuit would be dismissed on summary judgment since King is a public figure. In Britain, however, where there is no such doctrine, his lawsuit could go forward. In the United States there is a qualified privilege that serves as a defense to libel, where a party is under a legal, social or moral duty to communicate certain facts in the public interest. English law does not recognize a public policy-based defense in relation to public figures. Under the English law of defamation, an Internet web site would have the burden of verifying rumors about public figures.

In Internet defamation cases, a fair balance must be struck between the domestic tort law and rights of free expression. Information posted on the Internet may be protected in North America while violating contemporary community standards in less developed countries. An Islamic fundamentalist female might be publicly shamed by being depicted on a web site that shows her unveiled face. A Hindu might be humiliated by being placed unwittingly in a hamburger chain's online advertisement. Even within the Anglo-American tradition, there is sharp divergence in defamation law. The United States has carved out special tort rules making it difficult for public officials or public figures to sue for defamation. Due to stronger American protections for free speech, a plaintiff with a transatlantic reputation in both the United States and the United Kingdom will find obvious advantages in bringing a defamation suit in the United Kingdom. In Dow Jones & Co. vs. Harrods, for example, The Wall Street Journal was the defendant in a United Kingdom lawsuit over its republication of an April Fool's Day prank press release that was disseminated by Harrods Department Store on its web site and print editions. The English firm had issued a mock press release stating that it planned to float its department store by building a ship version of the store and offered to sell shares in the venture. Upon learning that the announcement had been a prank, the Journal countered with a story stating: *"If Harrods, the British luxury retailer ever goes public, investors would be wise to question its every disclosure"*. Harrods and its owner, Al Fayed, filed suit in London's High Court of Justice seeking damages for libel. Dow Jones, the owner of the Wall Street Journal, filed for a declaratory judgment, seeking to preclude the plaintiffs from pursuing their defamation claims.

Unlike Europe, there is no real codification of privacy rights in US law[163]. The framers of the US Constitution did not explicitly address privacy as a

163 www.jhtl.org/V5N1/04_JHTL_Lambert_RustadKoenig.pdf

fundamental right. The American law of privacy has evolved in piecemeal statutes at the federal and state levels. The path of US privacy law has been to limit governmental intrusion into a sphere of personal conduct and relations by defining the boundaries between the individual and the government.

With the rise of the Internet, national variations in substantive tort law become increasingly important. The privacy rights of the individual vary significantly under different legal regimes. French law, for example, differs markedly from US privacy-based torts. While the public activities of such persons necessarily subject more of their lives to legitimate public scrutiny, a public official or figure may shield from inquiry and intrusion those aspects of private life not related to the conduct of the public activities. Under French law, public officials and public figures may choose to protect their autonomy by withdrawing personal information previously divulged from the public arena and its return to the private domain.

In a United Kingdom case, the court ruled that sharing of personal information on an electoral register was a violation of the European Union Data Protection Directive. In Robertson v. Wakefield Metropolis Council, the plaintiff filed suit against his local election authority over the disclosure of personal information on the electoral register. The UK's highest court held that the local governmental authority violated both the UK Data Protection Directive and the European Convention on Human Rights by disclosing personal information.

The European approach to Internet privacy is a command and control model with precise rules governing the handling of personal information, in sharp contrast to the US legal system that relies largely upon a market-based solution to privacy. The European Data Protective Directive is designed to create uniformity in the processing of personal information across member states. This Directive gives data subjects control over the collection, transmission, or use of personal information. Moreover, the data subject has the right to be notified of all uses and disclosures about data collection and processing. A company is thus required to obtain explicit consent as to the collection of data on race/ethnicity, political opinions, union membership, physical/mental health, sex life, and criminal records[164].

The European Data Protection Directive requires that personal information be protected by adequate security. Data subjects have the right to obtain copies of information collected as well as the right to correct or delete personal data. It is important that consent be obtained from the data subject prior to entering into the contract. Personal data may not be transferred to other countries without an adequate level of protection. Member States are required to provide that a transfer of personal data to a third party takes place only if there is assurance of an adequate level of data protection. A company is

164 lsr.nellco.org/cgi/viewcontent. cgi?article=1006&context=suffolk/ip

liable for civil or criminal penalties for the unlawful processing of personal data. Damages may be assessed for the collection or transmission of information without a data subject's consent.

The European Union Data Protection Directive thus seeks to establish a regulatory framework that guarantees free movement of personal data. However, each individual is guaranteed a basic level of privacy by requiring each provider or transmitter to adhere to a set of guidelines.

In contrast, the United States prefers that the business community develop industry standards, such as a transnational online "privacy seal" that can be earned by adherence to industry norms. The European Data Protection Directive, on the other hand, requires Member States to assure that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection. No transfers of personal information of Europeans may be made to countries not having an adequate level of protection and complying with the notice and choice principles. Few sectors of the US economy comply with the minimum data protection principles required by European Data Protection Directive. The United States Commerce Department negotiated a safe harbor with the European Union by agreeing to adhere to reasonable precautions protecting data integrity. In the long term, the United States has no choice but to harmonize their data collection policies with those of the European Data Protection Directive.

The Loopholes

Internet law must become a moving stream rather than a stagnant pool, evolving to meet the new risks and dangers in the twenty-first century's age of information. Further harmonization between Europe and America is essential to surmount the growing substantive and procedural barriers to cross-border Internet-related tort litigation. Global Internet law[165] must develop effective mechanisms to facilitate cross-border enforcement of national judgments. Just as the leading Western nations cooperated to create a unified Law of the Sea, advances in cyber-space technology are creating international problems that need to be addressed through a coherent cross-national legal regime.

In 1982, the United Nations Convention on the Law of the Sea produced the first international agreement on developing principles of navigation, conservation, pollution, transit passage, and marine scientific research. This Treaty, signed by 147 nation states, resolved the plethora of conflicting claims by coastal States "*with universally agreed limits on the territorial sea*". A Law of Cyber-Space could be modeled on the mandatory system of dispute settlement adopted for the Law of the Sea.

Travelers on the World Wide Web require uniform[166] procedural and substantive remedies for cross-border civil wrongs. Similarly, the international

165 http://www.corbinball.com/articles_legal/index.cfm?fuseaction=cor_av&artID=947
166 http://www.policy.hu/bayer/ResearchPaper1.rtf

business community will be handicapped if it is subject to multiple conflicting procedural and substantive ground rules. Cross national trade requires a large degree of legal uniformity[167], and settled expectations about the rules of commerce and the processes by which those judgments are enforced.

A focus on the unique features of Internet Law is justified by the enormous impact of cyber-space on everyday life. Our transformation from a non-computerized world to one in which virtually all business, professional and entertainment activities are influenced, if not dominated, by electronic information systems has occurred rapidly. Hardly a day goes by without a court decision extending traditional civil law to adjudicate a cyber-space dispute. Cyber-space is too important, both economically and culturally, to simply allow market forces to shape its development.

Another possible approach to jurisdiction would be for the United States to enter into a treaty with the European Community countries, which would make the Brussels Regulation the prevailing rule. The Brussels Regulation generally endorses a freedom of contract in commercial contracts, but provides special protections for consumers. American consumers would greatly benefit from the Brussels Regulation because it designates choice-of-law, choice-of-forum and jurisdiction in the consumer home court. US companies operating in any country of the European Union are already subject to the Brussels Regulation's consumer rule. An American company domiciled in a Member State can be sued in that state. American online providers have been steadfastly opposed to the Brussels Regulation because they favor mass-market licenses, which require consumers to litigate in their home court and according to their home rules.

The Hague Convention will apply to most civil and commercial judgments but does not address disputes over revenue, customs, or administrative matters covered by other bodies of law. As with the Brussels Regulation, the Convention permits parties to choose their own forum. If the exclusive forum is in a nation state that is not a Hague Convention signatory, courts in contracting states should either decline jurisdiction or suspend proceedings.

Any future convention must enforce a broad range of judgments[168]; it must give courts the discretion not to enforce judgments which are considered to be obviously incompatible with the public policy of a country.

Europe's community-wide directive and convention approach is one possible model for harmonizing substantive Internet law. Directives have the virtue of creating uniformity in terms of basic principles, while permitting local variations to be incorporated into the law. As a result, each Member State of the European Community follows a dual system of regulation: European-wide rules and national variants. European Union regulations tend to be more rule-oriented than US law. The purpose of uniform laws throughout Europe is to

167 http://www.Internetatty.com/articles/liability.html
168 http://cirsfid.ing2.unibo.it/tfg-lea/meeting04/11ceve.pdf

facilitate commerce and reduce transaction costs in cross-border e-commerce. The United States is experimenting with adopting some features of European cyber-space law. America, for example, has joined eleven European nations in a pilot project to use ombudsmen to mediate Internet disputes. The Consumer Ombudsman will monitor the development of consumer problems connected with electronic commerce and work together with officials in other countries to develop common solutions.

The Law of Cyber-Space could progress by adopting tort concepts that permit consumers to redress injuries against powerful corporate stakeholders. The first step toward harmonizing cyber-tort law is to agree upon the broad principles of what constitutes a legally protected interest on the Internet. Without an international agreement to protect personal, property or reputational interests, cyber-wrongs will continue undeterred.

The Suggested Solution

The Internet has produced a network of user groups, bulletin boards, and web sites that have constructed a new arena where political and social norms are proposed, debated, and determined. It is no exaggeration to state that the content on the Internet is as diverse as human thought. Such ground-breaking advances in communications technology have always required the reworking of legal doctrine.

Regulatory and common law must be fundamentally re-shaped because the Internet is shattering the existing pattern by redefining distance, time, privacy and the meaning of territoriality. For example, it could be recommended that any person who registers a domain name that consists of the name of another living person, or a name substantially and confusingly similar thereto, without that person's consent, and with the specific intent to profit from such name by selling the domain name for financial gain to that person or any third party, should be liable in a civil action by such person. As a consequence, in any civil action a court may award injunctive relief, including the forfeiture or cancellation of the domain name or the transfer of the domain name to the petitioner. The court may also, in its discretion, award costs and attorneys fees to the prevailing party. This would become possible only after an agreement on a Law of Cyber-Space.

Internet technology is different in several key respects from previous technologies, in particular insofar as the Internet freely provides any-to-any communication. The types of substantive law more likely to be infringed by using on-line facilities include the following:

- Copyright material: The infringing act may occur when certain files containing copyright material such as text, pictures, or sounds are posted on a web page from which they may be downloaded all over the world.

- Illegal and harmful content: The infringing act may occur when material such as pornographic, racist or terrorist materials are disseminated via Internet facilities.
- Private and defamatory material: Private material such as pictures taken in intimate situations could be posted on web pages, bulletin boards, chat rooms, etc., and made available to users, thus infringing rights of privacy, including those contained in European data protection laws. The same may occur with defamatory material.
- Misrepresentation: This may occur when false or incorrect information is disseminated over on-line facilities, and causes damage to a third party.
- Others: An intermediary could also be held liable for the infringement of other substantive laws such as patents, trademarks, and unfair trade practices.

One can distinguish two basic types of liability standards [169] that may apply on-line. The standard may differ depending on the role, and may be different according to whether the party whose rights have been violated seeks damages or an injunction.

- Strict liability: According to this standard, on-line intermediaries will be held liable whenever a right is violated, i.e., whenever infringing or illegal material is disseminated using their facilities, whether they know (or have reason to know) about it and can control it or not. The imposition of the obligation upon on-line intermediaries to monitor the material passing through their systems would be equivalent to imposing strict liability upon them.
- With-fault liability: According to the with-fault standard, on-line intermediaries would be held liable whenever they intentionally or negligently violate the rights of others.

As mentioned in Toward a Universal Order of Cyber-Space: Managing Threats from Cyber-crime to Cyber-war - Report & Recommendations of the World Federation of Scientists, Permanent Monitoring Panel on Information Security [170], Recommendation 8, "*In parallel, to the elaboration and harmonization of national criminal codes, there should also be an effort to work toward equivalent civil responsibility laws worldwide. Civil responsibility should also be established for neglect, violation of fiduciary duties, inadequate risk assessment, and harm caused by cyber criminal and cyber terrorist activities.*"

Such an application of the established body of International Private Law expressely to cyber-space would be most helpful.

169 www.droit.fundp.ac.be/crid/xxeme

170 www.apdip.net/documents/access/ security/wfs_cybersecurity082003.pdf

CHAPTER 19. CIVIL REMEDIES

The Problem

As encountered by the average person, civil law is broken into two general subdivisions: contracts and torts. Contract law addresses written or oral agreements that are in dispute or have been breached in some manner. Torts are wrongs or harms that have been inflicted by one person upon another, either intentionally or through negligence.

Rather than prohibit specific acts, civil law deals with interpretation of agreements and events in order to discern what the reasonable conduct of the parties in a given situation should have been. The lawsuit is brought in the name of the plaintiff. If a defendant is deemed to have acted unreasonably, for example, broken a contract or caused intentional damage to property, then he may be subject to various remedies to restore the victim to a whole position, including the specific performance of a contract or monetary damages for breach of contract. Incarceration cannot be ordered by a civil court. The proper purposes of civil law are generally stated as compensation for actual damages suffered by the victim and, in cases of intentional wrongs, where both compensatory and punitive damages are recoverable, compensation and deterrence.

It has always been possible to try many criminal offenses in both criminal and civil court at different times or at the same time[171]. This allows the victim to access both types of remedies against a guilty defendant, that is, both imprisonment and compensation for damages. It should also be noted that the criminal law[172] does provide for an order of restitution, whereby the court orders the defendant to reimburse the losses suffered by the victim.

For several resons, civil procedures allow victims to prevail more often than do criminal ones for several reasons. There is no presumption of innocence. In criminal court, guilt must be established beyond a reasonable doubt; that is, it must be a virtual certainty that the defendant is guilty. In civil court, liability is established by a preponderance of the evidence; that is, it is more likely than not that the plaintiff's account is accurate.

The standards of evidence in civil court are thus lowered; for example, certain types of hearsay evidence are admissible, and more weight is placed on syndromes such as posttraumatic stress syndrome.

Constructing civil remedies[173] and criminal laws to deal with the misuse of cyber-space has always presented conceptual and practical difficulties for the law. Much has been done in recent years with respect to protecting personal data against interference, but much remains to be done in the area of confidential commercial information. It is clear that whilst the economic value

171 http://foreign.senate.gov/testimony/2004/HolleymanTestimony040609.pdf

172 Cyber-crimes by Damon W.D. Wright

173 Predicting The Future: Personal Jurisdiction For The Twenty-First Century Katherine C. Sheehan

of such information may justify its legal protection, its very nature makes the application of legal principles problematic. The approach to civil liability for misappropriation in common law has sought to avoid these complications by adopting an indirect approach to protection, focusing on the enforcement of obligations of confidence arising in law or equity in relation to such information rather than the information itself.

The Internet's blurring of national boundaries creates a variety of new civil remedies (cyber-tort) dilemmas. The global Internet's legal environment makes it inevitable that one country's laws will conflict with another's, particularly when a web surfer in one country accesses content hosted or created in another country. National differences among the cyber-tort regimes of different countries connected to the Internet will inevitably lead to conflicts of law. Which court will seize the case is one issue; which law will be applied is another.

Traditional concepts of jurisdiction and enforcement of judgment need to be adapted to the Internet. Transnational cyber-torts have yet to address cross-border Internet tort injuries such as the invasion of privacy, computer hacking, releasing viruses or worms, denial of service attacks, and other vulnerabilities unknown before the Internet.

No comprehensive treaty or convention sets the ground rules for cyber-tort causes of action, Internet remedies, the means for obtaining jurisdiction, or the enforcement of judgments[174].

Presently, almost no case law covers international Internet jurisdiction, and no statutory solutions exist to answer the question of cross-border Internet jurisdiction. It is theoretically possible for a business to be sued in hundreds of forums in foreign countries for the same course of online conduct, but this has not yet happened due to the difficulties in filing cross-border lawsuits. As businesses use the border-defying Internet, they will increasingly become subject to conflicting procedural and substantive law.

Common law countries and civil law countries have fundamentally different legal traditions that reflect their unique national histories. The common law approach of creating law around precedent is found only in the Anglo-American legal tradition. Despite the dominance of civil codes that are derived from Roman law, there are many national differences in all of the continental European countries. Sweden and Norway for example, have a well-established ombudsman tradition for resolving disputes, which does not exist in France. In the field of products liability, there are several divergent doctrinal paths that have survived the European Community's adoption of a Products Liability Directive. The European Community is seeking greater harmonization through the use of Directives, which are broad legal principles that require implementing legislation in each individual Member State. The countries that

174 www.jhtl.org/V5N1/04_JHTL_Lambert_RustadKoenig.pdf

follow the Anglo-American common law tradition share much common ground, but there are substantial differences even within their shared legal heritage.

Divergent Defamation Regimes is a common law tort action when a false oral or written statement has been made that lowers the plaintiff's reputation in the community. The Internet raises complex substantive legal conflicts as to what constitutes a defamatory statement and how reputation is to be measured in Internet transmissions. With hundreds of countries connected to the Internet, it is unclear whose standards apply. The English definition of defamation was a communication to a third person that tends to hold the plaintiff up to hatred, contempt, or ridicule, or to cause him to be shunned or avoided. What would be considered to be defamatory in England may be protected expression in the United States.

In Internet defamation cases, a fair balance must be struck between domestic tort law and the rights of free expression that vary between countries. Information posted on the Internet may be protected in North America while violating contemporary community standards in less developed countries. An Islamic fundamentalist female might be publicly shamed by being depicted on a Web site that shows her unveiled face. A Hindu might be humiliated by being placed unwittingly in a hamburger chain's online advertisement. Even within the Anglo-American tradition, there is sharp divergence in defamation law. The United States has carved out special tort rules making it difficult for public officials or public figures to sue for defamation.

Due to stronger American protections for free speech[175], a plaintiff with a transatlantic reputation in both the United States and the United Kingdom will find obvious advantages in bringing a defamation suit in the United Kingdom.

Since October 1998, the European member states have been enacting national privacy statutes to comply with the Data Protection Directive. In sharp contrast to the US legal system that relies largely upon a market-based solution to privacy, the European approach to Internet privacy is a command and control model with precise rules governing the handling of personal information. The European Data Protective Directive is designed to create uniformity in the processing of personal information across member states. This Directive gives data subjects control over the collection, transmission, or use of personal information. Moreover, the data subject has the right to be notified of all uses and disclosures about data collection and processing. A company is required to obtain explicit consent as to the collection of data on race, ethnicity, political opinions, union membership, physical andmental health, sex life, and criminal records.

The Data Protection Directive also requires that personal information be protected by adequate security[176]. Data subjects have the right to obtain copies

175 Criminal versus Civil Remedies for Intentional Wrongs by Wendy McElroy, August 13, 2004
176 The Legislative Response to the Evolution of Computer Viruses by: Mark R. Colombell

of information collected as well as the right to correct or delete personal data. Personal data may not be transferred to other countries without an adequate level of protection. Member States are required to provide that a transfer of personal data to a third party takes place only if there is assurance of an adequate level of data protection. A company is liable for civil or criminal penalties for the unlawful processing of personal data.

Damages may be assessed for the collection or transmission of information without a data subject's consent. The European Union Data Protection Directive seeks to establish a regulatory framework that guarantees free movement of personal data. However, each individual is guaranteed a basic level of privacy by requiring each provider or transmitter to adhere to a set of guidelines. In contrast, the United States prefers that the business community develop industry standards itself, and also seeks to develop a transnational online privacy seal that can be earned by adherence to industry norms.

The Data Protection Directive requires member states to ensure that the transfer of personal data to a third country may take place only if the third country in question ensures an adequate level of protection. No transfers of personal information of Europeans may be made to countries not having this adequate level of protection, and organizations are required to ascertain whether third parties subscribe to the principles of the Directive before transferring information to them. Few sectors of the US economy comply with the minimum data protection principles required by European Data Protection Directive. The United States Commerce Department negotiated a Safe Harbor with the European Union by agreeing to adhere to reasonable precautions protecting data integrity. The European Commission required US companies to adopt adequate level of protection for the privacy of individuals. The United States has no long-term choice but to harmonize their data collection policies with the European Data Protection Directive.

Spam covers unauthorized bulk e-mail advertisements. An OECD Report estimates that worldwide cost to Internet subscribers of spam is in the vicinity of $ 12.5 billion a year. In many of the US spamming cases, the courts awarded damages as well as injunctive relief under causes of action based upon personal property torts. In one case the court found the commercial e-mail actions to constitute trespass to chattels as well as a violation of state and federal computer abuse laws as well other causes of action. The court calculated damages by charging the spammer $2.50 per thousand messages for a total of $337,500.

The European E-Commerce Directive requires ISPs to implement policies designed to track down spam e-mailers by requiring them to provide contact information such as a verifiable business address and other authenticating information. Austria, Denmark, Finland, France, Germany, Greece, Hungary, Italy Norway, Poland, and Romania had all adopted national anti-spam

legislation by 2003. The European Commission's Directive on Privacy and Electronic Communications applies to unsolicited e-mail sent to residents of all European countries. Other anti-spam initiatives include the Commissions Directives on Misleading Advertising, E-Commerce Directive and the Data Protection Directive. The Europeans have adopted a more consumer-friendly approach to regulating spam than the United States' deference to free market principles.

The Electronic Commerce Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States. The purpose of the Directive is to create legal framework ensuring the free movement of information services. Member States are required to develop national legislation implementing the E-Commerce Directive. Article 9 of The Electronic Commerce Directive affirms Member States' obligation to remove obstacles to the use of electronic contracts. The Directive also covers topics such as the liability of intermediary service providers, unsolicited commercial e-mail, and the prohibition of Internet-related surveillance.

This legal regime institutes ISP liability rules not only for torts but also for all types of illegitimate activities in cyber-space that are initiated by third parties on-line, for example, copyright piracy, unfair competition, misleading advertising, etc.. The European Union's Electronic Commerce Directive's notice, take-down and put-back regime would compel an ISP to remove tortuous or other objectionable material. The Directive supplements national takedown policies are already in force in some European countries.

When a violation of copyright occurs, the offender is subject to a jail sentence and monetary fine, the respective length and amounts of which are contingent upon the degree of infringement. Also, the civil remedy is measured by several factors: the number of infringing actions; the value of the copyrighted works; and the number of previous offenses by the infringer; the greater these factors, the more severe the punishment.

Copyright violations are still criminalized where illegal reproductions and distributions, including sharing, knowingly occur on a relatively grand scale, but may also be criminalized for even smaller degrees of infringement.

Remedies[177] are currently evolving to police new forms of misbehavior such as Internet fraud, on-line stalking, etc... For example, women have been targeted by cyber-stalkers aided and abetted by Internet search firms that sell personal information. Internet wrongdoers have harmed women by posting personal information on sadomasochistic web sites and by using new technologies to superimpose their victim's face onto pornographic pictures. Tort law is frequently the only defense that women have against stalking or threatening e-mail transmissions from ex-husbands, former boy friends, or

177 In Defense of Tort Law By Thomas H. Koenig and Michael L. Rustad

strangers. Similarly, torts have been used to punish those who use the Internet to recruit children for pornographic purposes. Tort remedies are essential because the criminal law often lacks the flexibility to deter and punish these forms of wrongdoing.

The Existing Texts

Europe's harmonized system of procedural and substantive law has its roots in the unifying principles of the 1957 Rome Treaty. The European Union formed new legal institutions to carry out its objective of transcending national borders. Member States are represented on the European Council, which drafts legislation for Europe as a whole. The European Commission is charged with developing a legal framework to advance free competition in the Single Market. The Commission has powers of initiative, implementation, management, and control, which allow it to formulate harmonized regulations. In the past decade, the Commission has approved Internet regulations such as the E-Commerce Directive, E-Signatures Directive, Distance Selling Directive, Data Protection Directive, Database Protection Directive, and the Copyright Directive.

Under the Data Protection Directive each party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection as set out in this chapter.

Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data Chapter II :

Basic principles for data protection Article 10 – Sanctions and remedies-Provision on enforcement of rights:

A. Contracting Parties undertake to adopt, in accordance with their legal systems, the measures necessary to ensure the application of this Treaty.

B. Contracting Parties shall ensure that enforcement procedures are available under their law so as to permit effective action against any act of infringement of rights covered by this Treaty, including expeditious remedies to prevent infringements and remedies which constitute a deterrent to further infringements.

Diplomatic Conference on Certain Copyright and Neighboring Rights Questions

Article 14 - Provisions on Enforcement of Rights

Sanctions and measures

A. Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 - 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

B. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

Council of Europe Convention on Cyber-crime

Chapter II - Measures to be taken at the national level Section 1 - Substantive criminal law Title 5 - Ancillary liability and sanctions Article 13 - Sanctions and measures

Implementation

i. Member States shall provide appropriate remedies in respect of infringements of the rights provided for in this Directive.

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

Chapter IV- Common Provisions Article 12 – Remedies

ii. Member States shall determine the sanctions applicable to infringements of national provisions adopted pursuant to this Directive and shall take all measures necessary to ensure that they are enforced. The sanctions they provide for shall be effective, proportionate and dissuasive.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')

Article 20 – Sanctions and remedies

A. Member States 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.

B. Each Member State shall take the measures necessary to ensure that right holders whose interests are affected by an infringing activity carried out on its territory can bring an action for damages and/or apply for an injunction and, where appropriate, for the seizure of infringing material as well as of devices, products or components referred to in Article 6(2).

C. Member States shall ensure that right holders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right.

The Loopholes

New torts[178] may soon be on the Internet horizon. A few states have already recognized the tort of spoliation of evidence, punishing defendants that concealed their misconduct by destroying or altering smoking gun records. The spoliation remedy will be increasingly needed because of the ease with which electronic records can be altered, manipulated, morphed, or destroyed. The modus operandi of Internet wrongdoers frequently involves the use of pseudonyms, false identities, forged e-mail addresses, and encryption to conceal their activities.

Traditional tort actions are being used to confront these new dangers. The ancient tort of trespass to chattels, which was originally employed to

178 Sophisticated New Tort Theories Michael L. Rustad

compensate for injuries to personal property, has been extended to intangible property interests in cyber-space.

Internet security is a substantive field where tort remedies need to be fortified. In July 2000, a hacker broke into a Medical Center's internal network and downloaded computerized admissions records for four thousand heart patients. The medical facility would be negligent if it failed to implement industry standard security protocols, for example, if the hospital did not have adequate firewalls or encryption. This security breach raises the question of whether the web site victim of hacker activity may be liable for its contributory or comparative negligence if the data of patients or other third parties is intercepted or altered. The broader liability question is whether a web site owes a duty to maintain a secure computer network. Tort law's remarkable capacity to adapt and evolve to meet new threats and dangers makes it an important institution of social control in cyber-space.

The first question the legislatures and courts must address regarding civil liability for computer virus damages is whether computer information should be considered legally protected property. In order to resolve liability issues, it must recognize the property value of computer information.

Other problems raised by civil litigation in tort law for computer virus damage are personal jurisdictional boundaries and causation. One possible solution to the civil questions raised by computer virus damage is that computer users assume the risk of computer virus infection by doing business electronically. However, this is not an adequate solution to a problem that can cause wide scale economic damage. The proper remedy can be found in negligence.

In jurisdictions that provide for civil remedies, victims of computer virus who have sustained damage to their legally protected property can maintain a civil tort action and bring suit under the appropriate criminal statute[179].

However, just because a victim can bring suit for damages does not mean the victim will recover anything. One problem facing a victim is pinpointing the culprit. Victims will not want to pursue civil damages against an individual computer virus author for several reasons. First, an individual computer virus author is hard to catch. Secondly, even if the author is caught, it is unlikely that the author has deep enough pockets to make it worth the time and effort to attempt a damages recovery through the court system. Therefore, potential plaintiffs must look to pin liability elsewhere. The most likely candidates for defendants are the employers of the tort lawbreaker who distribute the virus. Yet, these companies will only be held liable for the negligent acts of their employees done within the scope of employment.

Many private corporations do not want to report cyber-terrorist incidents to the authorities. It is embarrassing for a private corporation to have its

179 www.law.ubc.ca/files/word_documents

network's security breached. Also, this type of event causes negative publicity for the corporation. The corporation's competitors could use this information against them, and the corporation will most likely lose business or stock-holder confidence.

The Suggested Solution

Internet law must evolve to meet the new risks and dangers in the information age. Further harmonization[180] between countries around the globe is essential to surmount the growing substantive and procedural barriers to cross-border Internet-related tort litigation. Global Internet law must develop effective mechanisms to facilitate cross-border enforcement of national judgments. Just as the leading Western nations cooperated to create a unified Law of the Sea, advances in cyber-space technology are creating international problems that need to be addressed through a coherent and universal Law of Cyber-Space.

Internet law must harmonize and homogenize procedural and substantive tort principles. In 1982, the United Nations Convention on the Law of the Sea produced the first international agreement on developing principles of navigation, conservation, pollution, transit passage, and marine scientific research. This Treaty, signed by 147 nation states, resolved the plethora of conflicting claims by coastal States...with universally agreed limits on the territorial sea. A Law of Cyber-Space could be modeled on the mandatory system of dispute settlement adopted for the Law of the Sea. No elegant utopian solution to the conflicting procedural and substantive tort law is likely to ever emerge, as any convention on cyber-torts will never satisfy the interests and objectives of every interest group.

180 Tenth United Nations Congress On The Prevention Of Crime And The Treatment Of Offenders Vienna, April 2000

CHAPTER 20. CRIMINAL LIABILITY

The Problem

A new breed of crime has emerged over the past decades – Cyber-Crime. This term covers all sorts of crimes committed with computers, from viruses to worms to Trojan horses; from hacking into private email to undermining defense and intelligence systems; from electronic thefts of bank accounts to disrupting web sites.

The problem of criminalizing[181] these cyber-crimes is a question of how the law deals with new technologies. Sometimes, existing laws treat crimes that employ new technologies as different and deserving of special regulation (wire fraud, hijacking of airplanes), and other times it does not (forged checks, anonymous letters, even bomb threats). Lurking underneath this differential regulation is a complex symbiotic relationship between technology and law. Computer crime forces us to confront the role and limitations of criminal law, just as criminal law forces us to reconceptualize the role and limitations of technology.

Computers make it easier for criminals to evade the constraint of social norms (through pseudonymity and removal from the physical site of the crime), legal sanctions (the probability of getting caught may be reduced for similar reasons), and monetary cost (because the resource inputs necessary to cause a given unit of harm are much lower).

The term cyber-crime[182] refers to the use of a computer to facilitate or carry out a criminal offense. This can occur in three different ways. First, a computer can be electronically attacked through acts that involve:

- unauthorized access to computer files and programs;
- unauthorized disruption of those files and programs; and
- theft of an electronic identity.

The above crimes involve situations in which a computer itself is the object of an attack. A rather different type of computer crime occurs when a computer is the tool used for an offence. For example, a computer might be used to distribute child pornography over the Internet, or it might be used to create massive numbers of copies of a popular and copyrighted song.

Complicated insurance fraud, large check kiting operations, and other sophisticated forms of white collar crime rely on computers to run the criminal operation. In these cases, computers make it easier to carry out a crime in real space. In these circumstances, computers are tools that expedite traditional offenses.

181 http://wwwiz.com/issue13/f02.html

182 http://www.cnn.com/2003/LAW/02/06/findlaw.analysis.ramasastry.cyberlaw

1. Unauthorized Access[183] to Computer Programs and Files

Unauthorized access occurs whenever an actor achieves entry into a target's files or programs without permission. The actor may be a person or another computer, and the access may be achieved electronically (through passwords and other mechanisms) or physically (by, for example, breaking into a file cabinet and stealing a PIN). Electronic access is by far the more common threat, and it is perpetrated by those who steal passwords, use computers to generate random passwords until entry is accomplished, or use trap doors to enter a secure area. A trap door is a fast way into a computer program that allows program developers to bypass security protocols built into the program. Programmers and software manufacturers place trap doors in programs so that they can quickly modify the underlying code. But these doors also permit anyone with a modest level of computer sophistication to break into a computer, and run it in any way he or she sees fit. The crime of unauthorized access is one of simply invading another's workspace. Causing harm to the files or programs or using the data improperly, these are separate crimes.

There are several different targets for unauthorized access; broadly speaking, they may be categorized as crimes against the government, individuals, and commercial entities. Governments have vast information[184] on these computers, ranging from nuclear secrets to defense planning contingencies, from human intelligence to law enforcement information about criminal organizations. Unauthorized access to such material can pose severe security risks.

By contrast, unauthorized access to an individual's personal files presents a different set of harms. These harms are generally harms to privacy, as personal files contain private and intimate thoughts. These thoughts may be as personal as love letters, as banal as grocery lists, or as useful as unfinished drafts of articles. In all these cases, the computer thief gains access to that information without permission[185]. Unauthorized commercial access, by contrast, may place a company's propriety information and trade secrets at risk.

The different types of targets suggest that different motivations may be at stake for different crimes: to gain financial benefits (copyright theft, trade secrets), to benefit a foreign enemy (espionage), to gain personal satisfaction (to spy on a boyfriend or enemy), to thwart law enforcement (by obtaining identities of informants), to exact revenge (a fired employee who wreaks computer havoc). There may be other targets as well, such as hospitals and research institutions with important data.

If a criminal uses the fruits of unauthorized access, the results may be devastating. Military secrets could be turned over to terrorist rogue states,

183 http://www.mosstingrett.no/info/legal.html

184 http://islandia.law.yale.edu/isp/digital%20cops/papers/brenner_newcops.pdf

185 http://www.swiss.ai.mit.edu/6095/student-papers/fall98-papers/trespass/final.html

people's most private thoughts could be placed on the Internet for all to see, and a company's most cherished trade secrets could be given to rival firms. These are four separate types of activity, but each shares the common factor of unauthorized access combined with distribution of the information to others.

2. Unauthorized Disruption

Unauthorized disruption is the heart of what most people consider to be the cyber-crime. It occurs when an entity, without permission, interferes with the functionality of computer software or hardware. By now, the idiom is familiar, viruses, worms, logic bombs, Trojan horses, and denial of service attacks.

a) Viruses

A virus is a program that modifies other computer programs. The modifications ensure that the infected program replicates the virus. In other words, the original program (analogous to a healthy cell) is changed by the virus to allow the virus to multiply. Once infected, the program secretly requests the computer's operating system to add a copy of the virus code to the target program. Once that computer is connected to another computer, either through the Internet, direct computer connection, or even through a common floppy disk, the virus may spread beyond the original host computer. The harmfulness of a virus will depend on the additional codes placed in the virus besides the code for its self-replication.

b) Worms

A worm is a stand-alone program that replicates itself. Both worms and viruses self-replicate. But a virus requires human action, from downloading a specific file to placing an infected disk in a computer, while a worm uses a computer network to duplicate itself and does not require human activity for transmission.

c) Logic Bombs & Trojan Horses

A logic bomb tells a computer to execute a set of instructions at a certain time under certain specified conditions. Those commands could be benign (a nice message from the programmer each year on her birthday) or damaging. A logic bomb can lie undetected in software or hardware, ready to be detonated when a series of events unfolds. The bomb resides in each version of the software, and millions of copies might be sold, all ready to detonate at a certain time. With a logic bomb, instead of just assaulting one computer, an attacker can reach thousands or even millions at once.

A Trojan horse, by contrast, is a computer program that performs some apparently useful function that also contains hidden code that is malicious. The malicious code may introduce a virus or other computer bug, or it may permit unauthorized access by an outside user. Indeed, Trojan horses are the most common way in which viruses are introduced into computer systems. In general, the horses are placed in software programs, but they may also be placed in hardware.

d) Distributed Denial of Service

Distributed Denial of Service (DDOS) attacks overwhelm websites and stop them from communicating with other computers. To carry out a DDOS attack, a hacker obtains unauthorized access to a computer system, and place software code on it that renders that system a master. The hacker also breaks into other networks to place code that turns those systems into agents (known as zombies or slaves). Each Master can control multiple agents. In both cases, the network owners become third-party victims, for they are unaware that dangerous tools have been placed and reside on their systems. The Masters are activated either remotely or by internal programming (such as a command to begin an attack at a prescribed time) and are used to send information to the agents. After receiving this information, the agents make repeated requests to connect with the attack's ultimate target, typically using a fictitious or spoofed IP (Internet Protocol) address, so that the recipient of the request cannot learn its true source. Acting in unison, the agents generate a high volume of traffic from several sources. This type of attack is referred to as a SYN flood (SYN is the initial effort by the sending computer to make a connection with the destination computer). Due to the volume of SYN requests the destination computer becomes overwhelmed in its efforts to acknowledge and complete transactions with each sending computer. As a result, it loses all or most of its ability to serve legitimate customers–thus the term Distributed Denial of Service.

e) Bot Software

Viruses, worms, Trojan horses, and network intrusions are among the threats that security administrators worry about on a regular basis. A less familiar threat that could be just as dangerous is malicious *bot* software. A bot is a program that operates automatically as an agent for a user or another program. Hackers forward bots to victims and the software automatically infects vulnerable computers. The bots then wait for commands from a hacker, who can manipulate them and the infected systems without the knowledge of the legetimate owner. A hacker can install bots on multiple computers to set up *botnets* that can then be used for massive distributed-denial-of-service attacks. Network-security experts identify and shut down botnets with compromised hosts several times a day. Botnets can also be used for mass spam mailings, installing key-logging software that can steal victims' passwords and data, and compromising computers to prepare them for infection by future viruses. Bot software is already on many computers and is one of the big underreported problems in security. Bots take advantage of system vulnerabilities and various memory-management problems that allow malicious code to infect a system. E-mail attachments with mass-mailing worms can carry bots. In addition, hackers can send bots via chat, file-transfer mechanisms or other means.

3. Theft of Identity

Identity theft occurs when one's identity is wrongfully appropriated by another. These situations are computer versions of familiar crimes (physical theft of credit cards, forged letters, etc.); cyber-space simply makes them easier to commit. Other types of identity theft via computer, such as cross-site scripting, Internet protocol spoofing, and page-jacking, do not have clear real space analogues. Cross-site scripting occurs when code is placed into a website to force it to send out information against the will of its owners. With Internet protocol spoofing, a perpetrator, using software, impersonates a computer trusted by the victim. As a result, the attacker computer, believed by the victim computer to be a different, friendly computer, achieves entry into sensitive areas or even control of the victim computer by operating privileged protocols. Page-jacking occurs when a link, logo or other Internet address is reprogrammed to bring a customer not to the intended site, but to some other one.

4. Carrying out a Traditional Offense

For virtual crimes[186] to exist, cyber-crimes must differ from crimes in some material[187] respect. Both cyber-crimes and crimes involve socially unacceptable conduct for which we impose criminal liability, so the most likely source of material differences between them is the principles needed to impose this liability. If cyber-crimes differ in one or more material respects from crimes, the principles used to impose liability for crimes should not suffice to impose liability for cyber-crimes. If, on the other hand, the principles[188] we use for crimes can be used to impose liability for cyber-crimes, they cannot be distinct entities and considered as different type of crimes.

The Existing Texts

EUROPEAN UNION

The Council of Europe Convention on Cyber-crime reads as follows:

Section 1 - Substantive criminal law

Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 - Illegal Access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 - Illegal Interception

186 http://www.rbs2.com/ccrime.htm

187 Is There Such a Thing as "Virtual Crime"? by Susan W. Brenner

188 http://faculty.ncwc.edu/toconnor/293/293lect03.htm

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagInternetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4 - Data Interference

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 - System Interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 - Misuse of Devices

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:

a) the production, sale, procurement for use, import, distribution or otherwise making available of:

-a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Article 2-5

-a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2-5, and

b) the possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 - 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

Unauthorized access is emerging in many jurisdictions as the threshold offence[189] in the field of computer crime. This is not at all surprising, since access is the fundamental factual predicate for anything else that can be done with a computer. In any event, unauthorized access appears to be the basic building block of most other computer crimes. It is the least included offense in a hierarchical series of crimes that become progressively more serious as aggravating harms and culpability are added to the base offense.

189 Legal Aspects of Computer-Related Crime in the Information Society by Prof. Dr. Ulrich Sieber

Penal provision is of vital importance in protecting and preventing information technology from criminal activity. The perpetration itself might appear to be innocent, but illegal access to data or information can cause severe problems[190]. Whenever there is a suspicion of illegal access from system hackers, all data and programs have to be verified for irregularities and viruses.

As a result of the recommendations from the OECD and the Recommendation, and the Council of Europe Convention, many countries have made the unauthorized access to data or information liable to punishment.

AUSTRALIA

Federal legislation: The Cyber-crime Act 2001

The Cyber-crime Act 2001 amended the Criminal Code Act 1995 to replace existing outdated computer offences.

478.1 Unauthorized access to, or modification of, restricted data

1. A person is guilty of an offence if:

a) the person causes any unauthorized access to, or modification of, restricted data; and

b) the person intends to cause the access or modification; and

c) the person knows that the access or modification is unauthorized; and

d) one or more of the following applies:

(i) the restricted data is held in a Commonwealth computer;

(ii) the restricted data is held on behalf of the Commonwealth;

(iii) the access to, or modification of, the restricted data is caused by means of a telecommunications service.

Penalty: 2 years imprisonment.

2. Absolute liability applies to paragraph (1)(d)

3. In this section: restricted data means data.

a) held in a computer; and

b) to which access is restricted by an access control system associated with a function of the computer.

AUSTRIA

Privacy Act 2000, effective as of January 2000:

Section 10:

52. Administrative Penalty Clause

Provided that the offence does not meet the statutory definition of a punishable action within the relevant jurisdiction of the court nor is threatened by a more severe punishment under a different administrative penalty clause, a minor administrative offence shall be pronounced with a fine of up to S260.000. Parties who

1. willfully obtain unlawful access to a data application or willfully maintain discernable, unlawful, and deliberate access or

190 Toward A Criminal Law For Cyber-Space: Product Liability And Other Issues by Susan W. Brenner

2. intentionally transmit data in violation of the Data Secrecy Clause (15), especially data that were entrusted to him/her according to 46 and 47, for intentional use for other purposes or

3. use data contrary to a legal judgment or decision, withhold data, fail to correct false data, fail to delete data or

4. intentionally delete data contrary to 26, Section 7.

BELGIUM

The Belgian Parliament has adopted new articles in the Criminal Code on computer crime, in effect from February 2001. The four main problems of computer forgery, computer fraud, hacking and sabotage are made criminal offences. The following unofficial text in English is based on a June 2000 version.

IV. Computer Hacking

Article 550(b) of the Criminal Code:

1. Any person who, aware that he is not authorized, accesses or maintains his access to a computer system, may be sentenced to a term of imprisonment of 3 months to 1 year and to a fine of (Bfr 5,200-5m) or to one of these sentences.

If the offence specified above is committed with intention to defraud, the term of imprisonment may be from 6 months to 2 years.

2. Any person who, with the intention to defraud or with the intention to cause harm, exceeds his power of access to a computer system, may be sentenced to a term of imprisonment of 6 months to 2 years and to a fine of (BFr 5,200-20m) or to one of these sentences.

3 Any person finding himself in one of the situations specified and who either: accesses data which is stored, processed or transmitted by a computer system, or procures such data in any way whatsoever, or makes any use whatsoever of a computer system, or causes any damage, even unintentionally, to a computer system or to data which is stored, processed or transmitted by such a system, may be sentenced to a term of imprisonment of 1 to 3 years and to a fine of (BFr 5,200-10m) or to one of these sentences.

4. The attempt to commit one of the offences specified is sanctioned by the same sentences as the offence itself.

5. Any person who, with intention to defraud or with the intention to cause harm, seeks, assembles, supplies, diffuses or commercializes data which is stored, processed or transmitted by a computer system and by means of which the offences specified may be committed, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of (BFr 5,200-20m) or to one of these sentences.

6. Any person who orders or incites one of the offences specified to be committed may be sentenced to a term of imprisonment of 6 months to 5 years and to a fine of (BFr 5,200-40m) or to one of these sentences.

7. Any person who, aware that data has been obtained by the commission of one of the offences specified, holds, reveals or divulges to another person, or makes any use whatsoever of data thus obtained, may be sentenced to a term of imprisonment of 6 months to 3 years and to a fine of (BFr 5,200-20m) or to one of these sentences.

BRAZIL

Law no. 9,983 of July 2000 has been adopted covering provisions:

Entry of False Data Into The Information System.

Art. 313-A. Entry, or facilitation on the part of an authorized employee of the entry, of false data, improper alteration or exclusion of correct data with respect to the information system or the data bank of the Public Management for purposes of achieving an improper advantage for himself or for some other person, or of causing damages.

Penalty-imprisonment for 2 to 12 years, and fines.

Unauthorized Modification Or Alteration Of The Information System.

Art. 313-B. Modification or alteration of the information system or computer program by an employee, without authorization by or at the request of a competent authority.

Penalty-detention for 3 months to 2 years, and fines.

The penalties are increased by one-third (one terco) until one-half if the modification or alteration results in damage to the Public Management or to the individual.

CANADA

Canadian Criminal Code Section 342.1 states:

1. Every one who, fraudulently and without color of right,

a) obtains, directly or indirectly, any computer service,

b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly , any function of a computer system.

c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offence under paragraph (a) or (b) or an offence under section 430 in relation to data or a computer system, or

d) uses, possesses, traffics in or permits another person to have access to a computer password that would enable a person to commit an offence under paragraph (a), (b) or (c) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

DENMARK

Penal Code Section 263:

2. Any person who, in an unlawful manner, obtains access to another person's information or programs which are meant to be used in a data processing system shall be liable to a fine, to simple detention or to imprisonment for a term not exceeding 6 months.

3. If an act of the kind described in subsection 1 or 2 is committed with the intent to procure or make oneself acquainted with information concerning trade secrets of a company or under other extraordinary aggravating circumstances, the punishment shall be increased to imprisonment for a term not exceeding 2 years.

GERMANY

Penal Code Section 202a. Data Espionage:

1. Any person who obtains without authorization, for himself or for another, data which are not meant for him and which are specially protected against unauthorized access, shall be liable to imprisonment for a term not exceeding three years or to a fine .

2. Data within the meaning of subsection 1 are only such as are stored or transmitted electronically or magnetically or in any form not directly visible.

Penal Code Section 303a: Alteration of Data

1. Any person who unlawfully erases, suppresses, renders useless, or alters data (section 202a(2)) shall be liable to imprisonment for a term not exceeding two years or to a fine.

(2) The attempt shall be punishable.

Penal Code Section 303b: Computer Sabotage

1. Imprisonment not exceeding five years or a fine shall be imposed on any person who interferes with data processing which is of essential importance to another business, another's enterprise or an administrative authority by:

committing an offense under section 300a(1) or

destroying, damaging, rendering useless, removing, or altering a computer system or a data carrier.

(2) The attempt shall be punishable.

INDIA

The Information Technology Act, 2000 (No. 21 Of 2000)

Chapter XI, Offences

66.Hacking with computer system.

1. Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

2. Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

JAPAN

Unauthorized Computer Access Law

Law No. 128 of 1999 (in effect from February 2000)

(Prohibition of acts of unauthorized computer access)

Article 3. No person shall conduct an act of unauthorized computer access.

2. The act of unauthorized computer access mentioned in the preceding paragraph means an act that falls under one of the following items:

a) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another persons identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code);

b) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item);

c) An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication, any information or command that can evade the restriction concerned.

Article 4. No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.

Article 8. A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not more than 500,000 yen:

1. A person who has infringed the provision of Article 3, paragraph 1;

Article 9. A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen.

SOUTH AFRICA

The Electronic Communications And Transactions Act Of July 31 2002 (Act No. 25, 2002)

Chapter XIII, Cyber Crime

Unauthorized access to, interception of or interference with data.

86. 1. Subject to the Interception and Monitoring Prohibition Act, 1992 (Act No. 127 of 1993), a person who intentionally accesses or intercepts any data without authority or permission to do so, is guilty of an offence.

2. A person who intentionally and without authority to do so, interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective, is guilty of an offence.

3. A person who unlawfully produces, sells, offers to sell, procures for use, designs, adapts for use, distributes or possess any device, including a computer program or a component, which is designed primarily to overcome security measures for the protection of data, or performs any of those acts with regard to a password, access code or any other similar kind of data with the intent to unlawfully utilize such item to contravene this section, is guilty of an offence.

4. A person who utilizes any device or computer program mentioned in subsection (3) in order to unlawfully overcome security measures designed to protect such data or access thereto, is guilty of an offence.

5. A person who commits any act described in this section with the intent to interfere with access to an information system so as to constitute a denial, including a partial denial, of service to legitimate users is guilty of an offence.

Penalties

88. 1. A person convicted of an offence referred to in sections 37(3), 40(2), 58(2), 80(5), 82(2) or 86(1), (2) or (3) is liable to a fine or imprisonment for a period not exceeding 12 months.

2. A person convicted of an offence referred to in sections 86(4) or (5) or section 87 is liable to a fine or imprisonment for a period not exceeding five years.

SWITZERLAND

Penal Code Article 143bis: Unauthorized access to data processing system.

Anyone, who without authorization, and without the intent of procuring an unlawful gain, accesses a data processing system which are specially protected against unauthorized access, by electronic devices, shall be sentenced to imprisonment or fines.

UNITED KINGDOM

Computer Misuse Act 1990, Chapter 18

Unauthorized access to computer material:

1. A person is guilty of an offense if-

a) he causes a computer to perform any function with the intent to secure access to any program or data held in any computer,

b) the access he intends to secure is unauthorized, and

c) he knows at the time when he causes the computer to perform the function that that is the case.

2. The intent a person has to have to commit an offense under this section need not to be directed at:

a) any particular program or data,

b) a program or data of any particular kind, or

c) a program or data held in any particular computer.

3. A person guilty of an offense under this section shall be liable on summary conviction to imprisonment for a term not exceeding six months or to a fine not exceeding level 5 on the standard scale or to both.

A person is guilty of an offense under this section if he commits an offense under section 1 above (the unauthorized access offense) with intent

a) to commit an offense to which this section applies; or

b) to facilitate the commission of such an offense (whether by himself or by any other person); and the offense he intends to commit or facilitate is referred to below in this section as the further offense.

This section applies to offences

a) for which the sentence is fixed by law; or

b) for which a person of twenty-one years of age or over (not previously convicted) may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates Courts Act 1980).

It is immaterial for the purposes of this section whether the further offense is to be committed on the same occasion as the unauthorized access offense or on any future occasion.

A person may be guilty of an offense under this section even though the facts are such that the commission of the further offense is impossible.

A person guilty of an offense under this section shall be liable

a) on summary conviction, to imprisonment for a term not exceeding the statutory maximum or to both; and

b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

A person is guilty of an offense if -

a) he does any act which causes an unauthorized modification of the contents of any computer; and

b) at the time when he does the act he has the requisite intent and the requisite knowledge.

For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any and by so doing -

a) to impair the operation of any computer;

b)to prevent or hinder access to any program or data held in any computer;

c) to impair the operation of any such program or the reliability of any such data.

The intent need not be directed at-

a) any particular computer;

b)any particular program or data or program or data of any particular kind;

c) any particular modification or a modification of any particular kind.

For the purposes of subsection (1)(b) above the requisite knowledge is knowledge that any modification he intends to cause is unauthorized.

It is immaterial for the purposes of this section whether an unauthorized modification or any intended effect of it of a kind mentioned in subsection (2) above is, or is intended to be, permanent or merely temporary.

For the purposes of the Criminal Damage Act 1971 a modification of the contents of a computer shall not be regarded as damaging any computer or computer storage medium unless its effect on that computer or computer storage medium impairs its physical condition.

A person guilty of an offense under this section shall be liable-

a) on summary conviction, to imprisonment for a term not exceeding six months or to a fine not exceeding the statutory maximum or to both; and

b) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

USA

Federal legislation:

United States Code, Title 18. Crimes And Criminal Procedure

Part I -Crimes

Chapter 47-Fraud And False Statements

(As amended October 3, 1996)

Section 1030. Fraud and related activity in connection with computers.

Whoever-

1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of

the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains-

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602 (n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 USC. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer if the conduct involved an interstate or foreign communication;

3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

4) knowingly and with the intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the faud and the thing obtained consists only of the use of the computer and the value of such use is not more than $ 5.000 in any one-year period;

5) i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

ii) intentionally accesses a protected computer without authorization, and as a result of such conduct recklessly causes damage; or

iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)-

> *i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least USD 5,000 in value;*
>
> *ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;*
>
> *iii) physical injury to any person;*
>
> *iv) a threat to public health or safety; or*
>
> *v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;*

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

A) such trafficking affects interstate or foreign commerce; or

B) such computer is used by or for the Government of the United States;

7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.

Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section. This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State or of an intelligence agency of the United States.

Privacy is recognized as a legal right in most countries, but with some differences with regard to differences in legal and cultural traditions. Many countries are in the process of adopting privacy protection laws to assure compatibility with standards and obligations in international agreements or guidelines, now compounded by the concerns for the cyber-space technologies. The concern over privacy violations is now greater than at any time in recent history. Mechanisms for protecting privacy in cyber-space could also be based on self regulation, under which private industry and companies could develop codes of conduct and practices. In most countries such self regulations are working together with regulation in order to ensure an efficient privacy protection. The problem is to establish a balance between the two mechanisms.

The Loopholes

Cyber-space is a unique medium for three reasons. Firstly, and most importantly, the use of computers and other equipment is a cheaper means to perpetrate crime[191] . Criminal law must be concerned not only with punishing crime *ex poste facto*, but with creating *ex ante* barriers[192] to inexpensive ways of carrying out criminal activity. The idea is that law should strive to channel crime into outlets that are more costly to criminals. Cyber-space presents unique opportunities for criminals[193] to reduce their perpetration costs; the probability of success achieved by a given expenditure is greater. Accordingly, the law should develop mechanisms to neutralize these efficiency advantages.

Secondly, some neutralization techniques, however, risk punishing utility-producing activities. For example, encryption has the potential to further massive terrorism (which leads many in the law enforcement community to advocate its criminalization) but also the potential to facilitate greater security in communication and encourage freedom (which leads many others to push

191 Criminal Law in Cyber-Space by Neal Kumar Katyal

192 www.apnic.net/mailing-lists/ apple/archive/2004/07/msg00006.html

193 14th BILETA Conference: "CYBER-SPACE 1999: Crime, Criminal Justice and the Internet".

for unfettered access to the technology). This is a standard "dual-use" dilemma that the law encounters in regulation of technology. The problem arises when an activity has both positive and negative uses, and forbidding the act forfeits the good uses. Since much cyber-crime is carried out through the use of Internet Service Providers (ISPs). Criminal law should consider imposing responsibilities on these third parties because they can develop ways to make crime more expensive, and may be able to do so in ways that the government cannot directly accomplish. This may be difficult because ISPs will tend to be very conservative, and hence suppress too much speech in attempting to avoid liability. US law has struggled with this quite a bit in the areas of defamation and copyright infringement. While this may indeed be very complicated the fact remains that once ISPs provide a service they should also bear the liability.

Thirdly, and more generally, a host of thorny problems arise because most activities that occur in cyber-space are invisible to third parties, and sometimes even to second parties, such as the very website that is being hacked. In a type of space where crimes are invisible, strategies that focus on trying to prevent crime by maintaining public order are of limited utility. On the other hand, the danger of overly aggressive law enforcement is multiplied in cyber-space. Each new major cyber-crime leads law enforcement to push for changes to the technical infrastructure to create better monitoring and tracing. If these codes are hidden in private hardware, public accountability may be undermined. A similar point is true about enforcement by police; because police are invisible on the Internet, the potential for entrapment may be greater. The ultimate effect of this loss of police visibility may be to poison legitimate activity on the Internet because confidence in communication may be undermined. A man cannot be sure that he is talking to a friend, and not to a government interloper seeking to document a criminal case. Because the technology of law enforcement is not well understood among the public, citizens may fear the Internet, and its advantages will be stymied.

Nevertheless, the differences between crimes that take place in cyber-space and those that occur in real space should not obscure their similarities. For example, if crime in cyber-space is easier to commit due to technical prowess, then the law needs to begin to think about how to treat offline crimes that harness technical ability. Similarly, if acts in cyber-space portend criminal activity in real space, then this dangerous complementarity can, if sufficiently strong, justify punishing acts in cyber-space (an example might be electronic stalkers, who may graduate to stalking in real space). This notion goes against the standard idea that criminal punishment should be reserved only for acts that are harmful; the point here is not that a certain act is harmful by itself, but that it may lead to a harmful act. Preventing the former act is a mechanism the government may use to discourage the commission of the latter.

It would be irrelevant to analyze every cyber-crime in this context, firstly due to the differences between common law countries and civil laws countries.

But nevertheless we can address generally to this issue with some representative assertions:

What if, a participant in an online chat room used language another participant found offensive? Would that not fall within the definition of this crime? By typing in the message, would the perpetrator-participant not be using non-corporeal means to overcome another's volition and thereby subject the victim to acts which may be found objectionable? The new crime of rape might also encompass actions taken by those playing online games[194]; one player might be found to have used non-corporeal means to overcome another's volition and thereby subject the latter to simulated acts which the victim found objectionable. And the same could be true in the physical world, as well. What if one person cut ahead of another in a line waiting to buy movie tickets? Could not one characterize the act of cutting in line as a use of corporeal force which overcame the victim's volition (her desire to remain at that particular point in line) and subjected her to an action he or she finds objectionable, in the sense of losing their place in line? Because the redefined rape crime would have such a broad application, it would almost certainly be struck down as unconstitutionally void for vagueness. Can we conclude then, that extant principles of criminal liability are inadequate to address cyber-space phenomena such as virtual rape? It does and it does not. As this example demonstrates, we will not be able to impose criminal liability for all the varieties of misconduct that will erupt in cyber-space simply by broadening our definitions of extant offenses so they encompass both physical and virtual activity. We can use this technique to address certain kinds of misconduct that will manifest itself in cyber-space. The more closely analogous cyber-situated misconduct is to misconduct, which is traditionally understood as criminal, the easier it will be to utilize this approach. But as we move more and more of our activities into cyber-space, we will certainly see new kinds of misconduct emerging, misconduct that may have little in common with the behaviors or harms our current repertoire of traditional crimes were devised to address. For these emerging types of misbehavior, we certainly have to develop a new approach to imposing criminal liability[195].

There are at least two different ways we can go about developing a new approach to imposing criminal liability for cyber-situated misconduct:

- We can use existing principles to define new crimes that encompass this kind of misconduct; or
- We can devise new principles for imposing liability such as a distinct law of cyber-crimes. If our goal is to ensure that miscreants cannot exploit cyber-space and engage in socially unacceptable conduct with impunity, it may be easier to "create" a new crime than to "adapt" an

194 www.boalt.org/bjcl/v4/v4brenner.htm

195 www.law.duke.edu/journals/ lcp/articles/lcp60dSummer1997p23.htm

> existing one. We could, for example, make it a crime to use a computer-generated communication to maliciously inflict emotional distress on someone. In so doing, we implicitly recognize that the new domain of cyber-space can be used to engage in types of socially unacceptable conduct that have not been encountered before.

Cyber-space, however, offers a much broader venue for misconduct than did the telephone or other twentieth-century technologies. Indeed, cyber-space may force us to rethink many of our views about the permissibility of predicating criminal liability on actions, and results, which occur elsewhere than in the physical world.

Anglo-American criminal law has generally been loath to impose liability unless certain elements, most notably an outlawed act or omission and a resulting harm, manifest themselves in the physical world[196]. This accounts for refusal to impose liability for thought crimes, a hesitance based in part on the empirical difficulty of establishing liability for crimes such as imagining the king's death, and also on the notion that people should be free to entertain whatever thoughts they like, as long as they make no effort to translate them into action that could harm the citizens. Those who will oppose the invention of new crimes targeting misconduct peculiar to cyber-space are likely to cite thought crimes as the proper analogy for what occurs in cyber-space, and argue that because this is a domain that exists outside of and apart from the physical we should not impose criminal liability for what occurs there. This argument fails because thought crimes are not the proper analogy for the kinds of misbehavior that will occur in cyber-space.

A distinct law of cyber-crimes must be created for social policy reasons because there are sound reasons specifically to denounce cyber-situated misconduct. This can be done symbolically, to make it clear that even though cyber-space is a new world, it still expected to conform to the standards which are enforce in our old (physical) world.

This can also be done for pragmatic reasons: One could argue that cyber-situated misconduct warrants special treatment because cyber-criminals can inflict greater harm than their real-world counterparts. Someone who uses the Internet to perpetrate a fraud scheme, for example, may be able to defraud many more people than someone who uses the telephone to do so simply because telephones require simultaneous one-to-one communication whereas the Internet lets the perpetrator take advantage of distributed, automated interactions with hundreds or even thousands of victims. Another argument for according special treatment to cyber-criminals is the difficulty law enforcement officers and prosecutors face in bringing these offenders to justice. It can be very difficult to identify the perpetrator of online offenses and, even when the perpetrators are identified, it can be very difficult to bring

196 California Criminal Law Review

them to justice, given the evidentiary and jurisdictional problems that can arise[197]. We may decide that the greater potential magnitude of the harm inflicted by a cyber-criminal or the greater likelihood he or she will avoid prosecution are additive harms that require treating these offenders differently.

A distinctive criminal law for cyber-crimes is also needed to deter individuals from using computers or cyber-space to carry out unlawful activity. The premise here is that having special cyber-crime legislation emphasizes the seriousness with which society regards the use of cyber-space as a criminal tool and, in so doing, causes would-be offenders to assess the risks inherent in committing a cyber-crime, a process which deters at least some percentage of them from engaging in such activity. Simply enacting statutes which impose criminal liability, even when that liability speak of Draconian punishments, is unlikely to have a deterrent effect on law-breaking behavior. Effective deterrence is a combination of many factors, of which the most important is the likelihood, or more accurately the perceived likelihood, of being apprehended and punished.

The Suggested Solution

Legal measures play a dominant role in order to prevent specific illegal activities by educating and deterring users, sanctioning perpetrators and compensating victims. However, legal measures must not be restricted to criminal law but should also include civil and administrative regulations (for example with respect to civil liability of providers). In the field of criminal law they should not only cover adequate regulations but also enable effective prosecution, while at the same time being adequate safeguards for the human rights of suspects and witnesses.

Due to the international dimensions of computer crime it is obvious that this should be co-coordinated, harmonized or unified on an international or supranational level, and that we must negotiate a new law that seeks to:

- strengthen international mechanisms for addressing illegal actions, for example by creating a well-defined set of international minimum rules against illegal actions, such as hacking, computer fraud and copyright infringements;
- strengthen international mechanisms for addressing illegal content, for example by creating a well-defined set of international minimum rules for illegal content to be prosecuted and punished world-wide, such as child pornography, bestiality, the glorification of violence, hate speech as well as defamation of minorities and individual persons;
- encourage countries to define an adequate system of rules for the responsibility of Internet access providers and service providers, for example by creating a legal system so that in all countries service

197 www.ichrp.org/ac/excerpts/204.doc

providers must undertake reasonable efforts to erase illegal content on their servers when made aware of this content;

- encourage countries to establish national laws for the effective prosecution of computer crimes, especially with respect to the search and seizure of computer systems and international networks, the duties of witnesses (for example, to provide passwords or to decrypt files), wiretapping and accessing computer systems;
- address possible abuses of anonymity, and install an international system for lifting anonymity in cases of abuse, thereby requiring adequate legal safeguards for privacy rights;
- develop an international information network and other information systems with respect to the prosecution of illegal and harmful practices detected on the Internet ;
- foster co-operation among law enforcement agencies, with special respect to urgent measures for freezing data in international search and seizure procedures ;
- clarify issues of jurisdiction ;
- educate and train law enforcement agencies about cyber-crime and its prosecution.

In sum, pending progress towards a uniform or harmonized legal order for cyber-space, especially as regards criminal law and law enforcement, it is recommended[198] that the relevant UN body, or the WSIS examine the feasibility of, and possibly the initiation of, steps towards the negotiation of a universal code of behavior for governments and the private sector in cyber-space , which would be designed to impede hostile action against other countries and which would create the optimum conditions for preventing cyber attacks.

198 Recommendations submitted to the World Summit on the Information Society at its Tunis phase (16 to 18 November 2005) World Federation of Scientists Permanent Monitoring Panel on Information Security, Erice, August 2005.

CHAPTER 21. CRIMINAL PENALTIES

The Problem

The role of criminal law penalties is to provide a deterrent to anti-social conduct where civil law is inadequate. More important, criminal law can deter and punish anti-social conduct regardless of economic consequences or the relative means of the victim or perpetrator. The decision to prosecute and the investigative resources both come from the state, not the victim. Criminal law uses the most powerful sanctions available to protect the rights of the members of society with punishments that are determined and administered through a process that society accepts as fair and principled.

As such, effective criminal enforcement regimes [199] are critical to establishing trust in social and economic institutions, both in the physical world and online. As more and more people connect, the benefits presented by migrating offline activities online can only grow. Society will not receive all of the economic and social benefits that it might from information technology until that technology along with the right people, processes, and norms create a level of trustworthiness comparable to that in the physical world.

The growing danger of crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes.

Self-protection is not sufficient to make cyber-space a safe place to conduct business. Rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber-crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments must therefore examine their current statutes to determine whether they are sufficient to combat the kinds of crimes discussed in this report. Where gaps exist, governments must draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes.

Undeterred by the prospect of arrest or prosecution, cyber-criminals around the world lurk on cyber-space as an omnipresent menace against the financial health of businesses, against the trust of their customers, and as an emerging threat to nations' security. Headlines of cyber-attacks command our attention with increasing frequency. This is only the tip of the iceberg as countless instances of illegal access and damage around the world remain unreported.

Outdated laws and regulations, and weak enforcement mechanisms, create an inhospitable environment in which to conduct e-business within a country

199 http://www.mcconnellinternational.com/services/cyber-crime.htm

and across national boundaries. Inadequate legal protection of digital information can create barriers to its exchange and stunt the growth of e commerce.

Countries that provided legislation were evaluated to determine whether their criminal statutes had been extended into cyber-space to cover different types of cyber-crime: data-related crimes, including interception, modification, and theft; network-related crimes, including interference and sabotage; crimes of access, including hacking and virus distribution; and associated computer-related crimes[200], including aiding and abetting cyber-criminals, computer fraud, and computer forgery.

In some countries, unauthorized access is a crime only if harmful intent is present; in others, data theft is a crime only if the data relates specifically to an individual's religion or health, or if the intent is to defraud. Laws tend to be biased in favor of protecting public sector computers, and the penalties provided in updated criminal statutes vary widely.

Punishment entails something which is assumed to be unwelcome to the recipient, such as loss of liberty through incarceration, disqualification from some activity, or loss of something of value, such as money or time. In determining an appropriate sentence, judges not only have to comply with sentencing legislation, which sets the maximum penalties that can be imposed, but they also have to comply with principles which include the need to accommodate the aims of proportionality, incapacitation, deterrence, rehabilitation, and restitution. Applying these various aspects to the circumstances of cyber-crime cases raises some difficult legal and practical problems.

Proportionality in punishment is the modern form of retribution that means that the severity of punishment[201] should be commensurate with the seriousness of the wrong. In the case of cyber-crime this raises serious difficulties as the consequences of some types of offending can be devastating, such as the creation and release of a computer virus, and yet the conduct itself may involve no physical violence or even contact with other people.

Incapacitation simply means that because the offender is isolated from society, generally through imprisonment, he or she will be prevented from committing further crimes of the same or similar nature while in isolation. In the case of cyber-criminals, however, prison has sometimes allowed them to continue their activities, and there have been cases in which fraudulent scams and pedophile activities have been carried on from prisons through the use of prison computers and mobile telephones smuggled into prison. The other problem with incapacitation is that although offenders may not repeat their offence while in prison, they often re-offend immediately upon release.

200 Bringing the Cyber-Criminal to Justice An Essay for the Technologically Impaired Keith A.Carsten
201 www.esecurityplaInternet.com/prevention/article.php/3419211

In determining whether punishment is an effective deterrent for cyber-crime, evidence is needed of the extent to which individuals are aware of the possible punishments which may result from their criminal conduct; whether they understand the probability of detection, prosecution and conviction, and whether or not individuals are minded to act upon any such knowledge by modifying their propensity to commit crime. Unfortunately, serious doubts have been raised about these matters. Surveys of offenders have found that they rarely know what penalties govern their conduct, although the hacking community is often quite knowledgeable about the exploits of other hackers and how they have fared in the courts. As we have seen, the probability of conviction tends to be relatively low in these cases for a range of legal and evidentiary reasons. Finally, research has shown that offenders rarely make a rational decision to carry out their offence or to desist, based upon the possibility of being punished.

A further problem with achieving deterrence lies in the fact that many individuals believe that what they have done should not be illegal. Many cyber-criminals have claimed that they had no malicious intention but were simply motivated by curiosity. Some who have stolen software illegally have believed that it is their right to make use of anything that is provided online. The result is that cyber-criminals might simply not accept that what they were doing is wrong.

The Existing Texts

EUROPE

Convention for the Protection of Individuals With Regard To Automatic Processing of Personal Data.

Article 6: data processing personal information on such issues as political or sexuality *may not be processed automatically unless domestic law provides appropriate safeguards*. Article 7 provides for the protection of personal data. Article 12 of Chapter III deals with the same point, this time dealing with personal data crossing national boarders. Article 13 of Chapter IV deals with mutual assistance and cooperation between parties making way for each party to establish authorities of contact for the purpose of international cooperation.

Article 17 addresses the costs of such an adventure, stressing that the data subject not be charged. Article 16 allows for a refusal of a request for assistance only when the request does not comply with the convention, and/or it would *be incompatible with the sovereignty, security or public policy of the party by which it was designated*. Article 1 states the purpose *to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him*. Article 14 allows a resident living aboard to *exercise the rights conferred by its domestic law*. Article 11 states that nothing shall limit a part

from providing persons greater and wider measure of protection. Article 25 allows for no reservations to the convention.

Article 13 of Title 5 of Chapter II of the Council of Europe's Convention on Cyber-crime states that the parties must ensure that violation of the articles put forth is *punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty*.

Article 8 of Chapter IV of the Directive of the European Parliament and the Council on the harmonization of certain aspects of copyright and related rights in the information society states that *Member states shall provide appropriate sanctions and remedies in respect of infringements of the rights and obligations set out in this Directive*.

USA

The first US regulation is the 2002 Federal Sentencing Guidelines[202]. It provides a graduated scale for sentencing guidelines. The document states: "*The estimate of the loss shall be based on available information, taking into account, as appropriate and practicable under the circumstances"*, including market value, number of victims, scope, and duration of the crime. The document makes way for *Departure Considerations*[203], in other words *cases in which the offense level determined under this guideline substantially understates the seriousness of the offense*. Here, a greater penalty may ensue. Such instances in which this may be enacted include situations where there was attempt to damage physically, emotionally, or psychologically, or *non-monetary harm.* Consistently, room is made for those situations *in which the offense level determined under this guideline substantially overstates the seriousness of the offense*.

In the second US document **(**2002 Federal Sentencing Guidelines-Departure Considerations**)** intellectual property offenses are treated in the same vein as theft and fraud in that they *reflect the nature and magnitude of the pecuniary harm caused by their crimes.*

CHINA

China's Regulations on Computer Software Protection

Chapter IV -Legal liabilities. Article 25 states: *The amount of damage for an infringement of software copyright shall be fixed in accordance with the provisions of Article 48 of the Copyright Law of the People's Republic of China*. Article 23 stipulates that the violator will *according to circumstances, bear such civil liabilities as stopping the infringement, eliminating the ill effects, making an apology and compensating for the damages.*

The Loopholes

A number of problems seem to be present regarding forfeiture and restriction of use orders in reducing cyber-crime[204]. First, the use of forfeiture of an offender's personal computer and modem is unlikely to stop the offender

202 www.ussc.gov/GUIDELIN.HTM

203 www.ussc.gov/2002suppa/2b1_1.htm

204 Cyber Crime Sentencing The Effectiveness of Criminal Justice Responses Dr Russell G. Smith

from using any one of a number of computers that are readily available to members of the public in libraries and other public places such as Internet cafes. Forfeiture is, therefore, unlikely to have an incapacitating effect.

Secondly, forfeiture of a personal computer may affect individuals other than the offender, such as where other family members make use of the computer for school work or recreational activities. Forfeiture could, therefore, infringe the principle of proportionality in punishment.

Thirdly, restriction of use orders will only be effective to the extent that the order is capable of being enforced. This may require that probation officers be trained in computer forensics to conduct thorough inspections of the offender's computer, which is unlikely to be feasible for most probation services. Technologically adept offenders would be quite capable of concealing their activities from probation officers, most of whom who have not been fully trained in computer forensics.

Fourthly, if monitoring or filtering software is installed on the offender's computer this could be disabled by the offender, or be either inadequate to detect the full range of prohibited content, or, alternatively, could be over-inclusive and prevent the offender from gaining access to legitimate content. This could impede a person's potential rehabilitation or employment during parole.

Fifthly, forfeiture and restriction of use orders could create problems in terms of rehabilitation of offenders, particularly for individuals who work in the information and communications technologies industries where a ban on computer or Internet usage may make them unemployable. In addition, the use of filtering software may be over-inclusive and prevent the offender from gaining access to legitimate content.

Finally, and related to the problem of achieving rehabilitation, forfeiture and restriction-of-use orders may mean that the offender is unable to earn sufficient money to pay compensation orders or other financial penalties. Similarly, offenders subject to forfeiture or restriction-of-use orders could not engage in some types of constructive community service that might require the use of computers. In this sense, their skills are being wasted during the period of the order.

One of the major loopholes in regulating the cyber-space is the fragile criminal penalty bylaw[205]. Below are some of the characteristics that need to be addressed.

Despite the progress being made in many countries, most countries still rely on standard terrestrial law to prosecute cyber-crimes. The majority of countries are relying on archaic statutes that predate the birth of cyber-space and have not yet been tested in court.

205 Forgery in Cyber-Space: The Spoof could be on you! Stephanie Austria, Spring 2004

The weak penalties in most updated criminal statutes provide limited deterrence for crimes that can have large-scale economic and social effects.

The actual general weakness of statutes increases the importance of private sector efforts to develop and adopt strong and efficient technical solutions and management practices for information security.

Little consensus exists among countries regarding exactly which crimes need to be legislated against. Unless crimes are defined in a similar manner across jurisdictions, coordinated efforts by law enforcement officials to combat cyber-crime are complicated.

Most countries, particularly those in the developing world, are seeking a model to follow. These countries recognize the importance of outlawing malicious computer-related acts in a timely manner in order to promote a secure environment for ecommerce. But few have the legal and technical resources necessary to address the complexities of adapting terrestrial criminal statutes to cyber-space. Therefore a coordinated partnership to produce a model approach can help eliminate the potential danger from the inadvertent creation of cyber-crime havens.

The Suggested Solution

Extending the rule of law into cyber-space is a critical step to create a trustworthy environment for people and businesses. Since that extension remains work in progress, organizations today must first and foremost defend their own systems and information from attack, be it from outsiders or from within. They may rely only secondarily on the deterrence that effective law enforcement can provide.

To provide this self-protection, organizations should focus on implementing cyber-security. Organizations need to commit resources to educate employees on security practices, develop thorough plans for the handling of sensitive data, records and transactions, and incorporate robust security technology-such as firewalls, anti-virus software, intrusion detection tools, and authentication services, throughout their computer systems.

These system protection tools, the software and hardware for defending information systems, are complex and expensive to operate. To avoid hassles and expense, system manufacturers and system operators routinely leave security features turned off, needlessly increasing the vulnerability of the information on the systems. Bugs and security holes with known fixes are routinely left uncorrected. Further, no agreed-upon standards exist to benchmark the quality of the tools, and no accepted methodology exists for organizations to determine how much investment in security is enough. The inability to quantify the costs and benefits of information security investments leave security managers at a disadvantage when competing for organizational resources.

The methods that may be adopted are mainly three: (a) creation of particular definitions of crimes; (b) reinterpretation of the already existing crimes, with the purpose of mending the small gaps and together with the reinterpretation, and (c) the addition of some paragraphs to the already existing crimes in order to remedy the gaps.

In the light of the above the following improvements are suggested but are not limited to:

- International substantive criminal law regimes should be harmonized where practicable.
- Traditional crimes committed using computers or networks should generally be punished, when committed online, just as it they would be punished if committed in the physical world.
- When traditional crimes present a greater harm to society because they are committed online, that crime should entail a heavier punishment, where possible through neutral means such as measuring the actual damage done.
- Where the use of a computer or network inherently increases the risk or harm to society, criminal provisions should impose a greater or new punishment for such use unless the additional risk or harm is already addressed through neutral means.
- Criminal sanctions should where necessary deter costly anti-social conduct. Criminal sanctions should establish necessary ethical norms.
- The presence of technical or other solutions that could prevent the harm from network-related crime does not obviate the need for criminal sanctions.
- Criminal sanctions should help prevent unknowable or unbounded harms which cannot be otherwise be remedied.
- Criminal sanctions must apply to harmful misuse of identity online.

In conclusion, online substantive criminal law should avoid technology specificity, should enforce societal norms, and should deter anti-social conduct online just as criminal law does generally, and should impose punishments proportional to the damage the offense causes to the victim and to society at large.

CHAPTER 22. SOVEREIGNTY AND JURISDICTION

The Problem

As the community of Internet users grows exponentially and becomes increasingly diverse, geographic boundaries become more and more porous and ephemeral, and the range of on-line interaction expands. As that happens, disputes of every kind will occur. On-line contracts will be breached, on-line torts will be committed, on-line crimes will be perpetrated. Although many of these disputes will be settled informally, others may require formal mechanisms for dispute resolution.

Among the most serious questions raised by the need for Internet regulation are those relating to jurisdiction[206], or a tribunal's ability to subject an individual to adjudication in a particular forum. The geographic transparency of the Internet may well place such adjudication of trans-border disputes outside of any jurisdictional analysis as yet contemplated by territorially-bound law. Although problems of multi-jurisdictional coordination and competition are not unique to the regulation of the Internet, the peculiar nature of the Internet may trigger constitutional limitations which are designed to limit governmental jurisdiction within a state's physical borders.

Jurisdiction, defines three kinds of power: the power to prescribe, the power to adjudicate, and the power to enforce. The first of these relates principally to the power of a government to establish and prescribe criminal and regulatory sanctions; the second, to the power of the courts to hear disputes, especially civil disputes; and the third, to the power of a government to compel compliance or to punish noncompliance with its laws, regulations, orders, and judgments.

The challenge in determining if and when courts have jurisdiction over activities conducted on the Internet would not be great if the Internet were confined to a single geographical area, or if it were neatly divisible along territorial boundaries into distinct local networks.

The right of a country to exercise jurisdiction on the basis of the nationality of a defendant is universally recognized. A country is assumed to have nearly unlimited control over its nationals, so the treatment of its nationals is not ordinarily a matter of concern to other States or to international law. In the context of cyber-space, however, courts have yet to directly rely on nationality as a nexus for asserting jurisdiction.

Ordinarily, international law only applies to relations between nations. It is, first and foremost, inter-national law, or law between nations. As such, it normally does not establish regulations or criminal sanctions that apply directly to individuals. The exception to this rule is for the small category of crimes that are covered by the universality nexus; that is, those crimes that are considered

206 http://www.law.indiana.edu/fclj/pubs/v50/no1/wilske.html

to be so egregious as to be of universal concern. Because these crimes are established by international law (*delicta juris gentium*), and not national law, any court with competence to apply international law has jurisdiction to hear them. There is no requirement that the crime be related to the forum or its territory. The only requirement is that the forum must properly have the defendant in its custody.

The crimes covered by the universality nexus include, at least: piracy, the slave trade, attacks on or the hijacking of aircraft, war crimes, genocide, and crimes against humanity. This list, however, has been expanding since the end of the World War II. For example, the 1996 Draft Code of Crimes Against the Peace and Security of Mankind prepared by the International Law Commission includes an extensive list of acts that make up crimes against humanity, including murder, extermination, enslavement, torture, persecution on political, racial, religious, or ethnic grounds, rape, enforced prostitution, and sexual abuse when committed in a systematic manner or on a large scale and instigated or directed by a Government or by any organization or group, as well as a lengthy list of war crimes, including murder, torture, and terrorism.

To date there have been no cases in which the universality nexus has been applied to criminal conduct in cyber-space[207]. There has been a great deal of interest, however, in the topic, especially since the terrorist attacks of September 2001, and the US government's assertion of a global war on international terrorism.

The criteria for courts to assert jurisdiction over crimes and civil actions in cyber-space have begun to take some concrete form. In criminal and regulatory cases, the traditional nexuses used by courts to assume jurisdiction over international defendants, namely, territoriality, nationality, or protective and universality norms, all apply in cyber-space. At present, however, only the territoriality nexus has been directly invoked by the courts. This is likely to change as the number of cyber-cases increases.

In civil cases, both the common law world and the European Union are moving to assert *in personam* jurisdiction over merchants and consumers who complete transactions over the Internet. In the common law world, this requires a showing of a connection between the transaction and the forum. In the European Union, suits in consumer disputes are ordinarily brought in the consumer state of domicile, while non-consumer disputes are heard in the forum where the contract was to be performed. .

Civil *in rem* jurisdiction, which is consistently defined worldwide, is presently being used in German courts to assert jurisdiction over domain names, software, and other kinds of intellectual property. It seems likely that it will be used in the same way in other courts in the future.

207 stlr.stanford.edu/stlr/articles

While the criteria for courts (both national and international) to assume jurisdiction are quickly taking shape, and the pattern worldwide is reasonably consistent, the decisions that have defined those criteria have created problems, especially with respect to forum avoidance, retailer entrapment, tax cheating, and free speech.

Forum selection clauses are enforceable worldwide for almost all kinds of transactions. The exception is for consumer contracts. In the European Union, the clauses are unenforceable; while in the United States and elsewhere, they are enforceable[208]. These differing approaches are reflected in the Draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters, where the negotiating parties have yet to agree to a uniform treatment; and it looks as if they will include both approaches in the final convention.

Improved geo-location software looks to be the mechanism that courts and merchants will adopt for dealing with retailer entrapment and tax cheating. As for free speech, individuals and juridical entities may exercise it to the extent they are allowed to do so in their country of domicile provided they do not travel or establish overseas branches, agencies, or establishments.

However, justice systems have faced new questions concerning the conflict of state criminal laws. These new questions have old answers; the doctrine of constructive presence has established a state's authority to proscribe an out-of-state activity that has in-state effects. Beyond the mechanical application of jurisdictional rules, however, there lie deeper policy questions concerning the fairness of subjecting computer users to multiple, inconsistent bodies of law. Cyber-space exists in all jurisdictions, and in no particular jurisdiction, at the same time. There is an apparent tension between the free flow of cyber-space and the sovereignty of those territories which it touches.

Today, countries worldwide are learning that traditional domestic laws are inadequate when dealing with transnational cyber-crime, or in attempting to bring responsible persons on foreign soil to justice. It is evident that laws would have to transcend physical boundaries to remedy this ongoing problem.

Sovereignty is the exclusive right to exercise supreme authority over a geographic region, group of people, or oneself. Sovereignty over a nation is generally vested in a government or other political agency, though there are cases where it is held by an individual. A monarch who rules a sovereign country can also be referred to as the sovereign of that country. The concept of sovereignty also pertains to a government possessing full control over its own affairs within a territorial or geographical area or limit.

In international law, the important concept of sovereignty refers to the exercise of power by a state. *De jure* sovereignty refers to the legal right to do so; *de facto* sovereignty to the ability in fact to do so. Foreign governments may recognize the sovereignty of a state over a territory, or may refuse to do so.

208 www.itu.int/osg/spu/visions/papers/freepaper.pdf

There exist vastly differing views on the moral bases of sovereignty. These views translate into various bases for legal systems:

- Partisans of the divine rights of the kings, argue that the monarch is sovereign by divine right, and not by the agreement of the people. This, pushed to its conclusion, translates into a system of absolute monarchy.
- Most democracies are based on the concept of popular sovereignty: Ultimately, sovereignty is vested in the people, who freely grant the exercise of it to the government.
- Anarchists and some libertarians deny the sovereignty of states and governments.
- Supporters of democratic globalization consider that nation-states should yield some of their power to a world organization controlled by world citizens, instead of being organized on an intergovernmental basis as is the case at present.

The key element of sovereignty in the legalistic sense is that of exclusivity of jurisdiction. Specifically, when a decision is made by a sovereign entity, it cannot generally be overruled by a higher authority[209]. Further, it is generally held that another legal element of sovereignty requires not only the legal right to exercise power, but the actual exercise of such power. No *de jure* sovereignty without *de facto* sovereignty. In other words, sovereignty requires both elements, whether in the claim or proclamation of sovereignty, or in the exercise of sovereignty.

One can conclude that to avoid prosecution an individual may have to obey each of the following:

- The laws of the country that one is a national of;
- The laws of the country that one lives in;
- The laws of the country that one is in.

The Existing Texts

The fundamentals[210] of jurisdiction within European countries are based on statute or regulation. In the United States these same fundamentals arise out of law cases interpreting constitutional parameters. Despite their different perspectives, the results under both systems have a good deal in common.

In the European Union, the Brussels Convention has been the controlling document for jurisdictional issues. It sets forth the following basic rules:

First, a person who is domiciled in an EU member country may be sued in that country. Second, in contract matters, a person may be sued in the place of performance of the obligation in question. Third, in tort matters, a person may be sued in the place where the event causing harm occurred. Fourth, a

209 http://www.kentlaw.edu/cyberlaw/

210 www.inter-disciplinary.Internet/ci/mm/mm1/smith%20paper.pdf

consumer may be sued only in the consumer country of domicile, while a consumer may elect to bring an action in either his domicile or in the other party's domicile, so long as the consumer was subject to a specific solicitation or advertising in the consumer domicile. Finally, in contracts not involving a consumer, the parties can agree on a forum for disputes.

Since jurisdiction in European countries[211] is not limited by constitutional principles as it is in the US, the Brussels Convention does not require minimum contacts between the forum and the defendant. The Convention permits assertion of jurisdiction over a defendant if conduct wholly outside the forum resulted in a tortuous injury to the plaintiff within the forum.

In the United States, traditionally, there are two types of personal jurisdiction[212] which state courts may exert in the US: the general and the specific. In addition, a third jurisdiction is also relevant to cyber-space law, particularly with regard to ownership of domain names, namely, *in rem* jurisdiction.

a) General Jurisdiction.

General jurisdiction in the US allows a forum to take jurisdiction over a given person in disputes that do not necessarily relate to the forum. Accordingly, the criteria for the application of general jurisdiction under US constitutional due process limitations are very strict. Such jurisdiction can apply only if the defendant's contacts with the forum are systematic and continuous. General jurisdiction has been accorded less attention thus far than specific jurisdiction in the cases involving the Internet, but it may gain importance as eCommerce evolves.

b) Specific Jurisdiction.

Under US law, a given forum has specific jurisdiction over a defendant whose contacts with the forum relate to the particular dispute in issue. In 1945, the US Supreme Court held that personal jurisdiction over a non-resident defendant by a forum state requires only that, "*he has certain minimum contacts with it, such that the maintenance of the suit does not offend traditional notions of fair play and substantial justice*". Existence of the required minimum contacts is determined under a three-part test:

- The defendant must purposefully direct his activities or consummate some transaction with the forum state or a resident thereof; or perform some act by which he purposefully avails himself of the privilege of conducting activities in the forum and thereby invokes the benefits and protections of its laws;
- The claim must be one arising out of or relating to the defendant's forum-related activities; and

211 Shearer, I.A., Starke's International Law, (London; Butterworht, 1994)

212 http://www.richmond.edu/~jolt/v4i2/thornton.html

- The exercise of jurisdiction must comport with fair play and substantial justice,
- It must be reasonable.

c) *In Rem* Jurisdiction.

In rem jurisdiction involves jurisdiction over a thing rather than a person. Such jurisdiction gives the court the power to determine the rights of every person in the thing, such as issuing a judgment of title to land.

The principal difference arises from the contrast between the Rome Convention regarding consumer contracts and mandatory rules, which permits the enforcement against consumers of reasonable choice-of-forum clauses even in a contract of adhesion. Article 5 of the Rome Convention does not enforce the waiver by consumers of mandatory laws of their habitual residence designed for their protection, although a choice-of-law clause may apply different law to other aspects of the contract and dispute.

If there is no choice-of-law clause, Article 5 provides that the law to be applied is that of the consumer habitual residence, unless the contract is one for carriage (other than an inclusive contract for travel and accommodation) or for provision of services exclusively in another forum.

The EU Proposal is similar to the Rome Convention; it provides that: "*The autonomy of the parties to a contract other than an employment, insurance or consumer contract to determine the courts having jurisdiction must be respected. Contractual clauses electing jurisdiction between parties with unequal negotiating strength must, however, be regulated*".

Subsequently, it adds: "*with particular regard to choice-of-jurisdiction clauses in consumer contracts, a review of the planned system will be conducted after the entry into force of this Regulation in the light of developments in non-judicial dispute-settlement schemes, which should be speeded up*".

In the US, it is also possible, although not axiomatic, for public policy to override choice-of-law in consumer contracts. Nonetheless, the policy is invoked much more seldom than in Europe. As we recognize the dramatic change in the power parameters that the Internet creates between supplier and consumer, the notion that consumers are unable to make valid decisions on choice-of-law and forum becomes less defensible. Indeed, even default rules that make the consumer residence the proper forum for disputes arising from a retail transaction need reexamination. The EU members are still adhering to non-waivable consumer protection on choice-of-law, if not on choice-of-forum.

The Brussels Regulation arguably makes the ultimate outcome of the Hague Convention on Jurisdiction less important. The Hague Convention[213], which aims to make civil judgments enforceable across borders, has been

213 The Hague Convention on Jurisdiction and Foreign Judgements in Civil and Commerical Matters, art. 7(2), June 2001 (Working Revision) [hereinafter Hague Convention 2001]

stalled since 1999 due to a disagreement over how business-consumer disputes should be settled. This treaty would require US companies to defend consumer suits in the country where the consumer resides, even if the company did not intend to market to that forum, as long as the company advertised on the web. Moreover, unlike the present situation where US courts which are asked to enforce a foreign judgment will examine the jurisdiction of the foreign court using US standards of minimal contacts, the Hague Convention would require US courts to enforce foreign judgments as long as they simply satisfy the criteria of the Hague Convention.

Thus, under The Hague Convention, US courts would be required to enforce a foreign judgment against a US resident even if the only contacts with the foreign country were that its site could be accessed there. In addition, the Hague Convention would limit the choice of enforcement so that consumers may be enforced only when they are agreed upon after a dispute has arisen or when they permit the consumer to bring proceedings in another court[214]. The effect of the Convention would be to make a business vulnerable to suit anywhere on the world where its site is visible.

The Loopholes

Traditional law is based on the notion that activity occurs in a particular jurisdiction - a nation, a state/territory, a municipality - and can be dealt through reference to the rules (and authorities) of that physical location.

Some theorists have argued that we now live in a borderless world where people, capital, and information, permeate through jurisdictional boundaries at will. The Internet thus poses particular challenges. There may be questions about where online activity takes place. There may be questions about the location or nature of any dispute resolution mechanisms, since few regions have identical law. And there may be questions about the shape, authority and effectiveness of any regulatory enforcement, as even if police or lawyers are able to identify online malefactors; their power may stop at the border.

German law, for example, forbids Holocaust denial and the dissemination of Nazi propaganda. Far-right groups in Germany and other states publish such material from sites based outside German jurisdiction, including Australia and the US. German courts have responded by declaring that the publication of Nazi material on any site is an offence. In December 2000 the German Supreme Court upheld a conviction against Adelaide-based Frederick Toben.

In November 2000 French courts gave US-based Yahoo three months to prevent French citizens from accessing similar material, although such publication is allowed under US free speech provisions, and needless to say that French law does not apply in the US but many experts argue that technology would not permit any such differentiation.

214 www.howardrice.com/uploads/ content/jurisdiction_ecomm.pdf

While the US has used trade negotiations several times to enforce the extraterritorial application of its law, in Europe little case law concerning jurisdiction on the Internet has so far been established. Due to this, one inevitably has to turn to constitutional law. As most legal systems in Europe are civil law systems, solutions based on constitutional law cannot be neglected. Therefore, one has instead to look for more general international or national law covering issues of jurisdiction.

In cases of cross-border transactions, or in other cases with an international dimension, jurisdictional issues have traditionally been an issue for nation states to decide on, for example within the framework of international law[215]. This has also been the case in Europe, but during the last half-century such issues have increasingly become subject to international conventions and treaties as nation-states have increasingly realized the need for conformity.

Thus, the solution for Internet jurisdiction issues would be to make a thorough analysis of the changes and amendments called for by the new situation. Criminal law is an area where countries have traditionally been reluctant to conclude conventions and treaties concerning jurisdictional issues, and cooperation is generally limited. Each country obviously wishes to determine by itself which criminal laws to enact and how to exercise its jurisdiction[216] to enforce these laws. Compared with commercial law, little has been done to regulate jurisdictional issues within an international setting.

The Suggested Solution

A conclusion that can be drawn from the cases discussed above is that present International Law[217] already provides a base for solutions to problems concerning jurisdiction over crimes committed over the Internet. What is needed is greater co-operation among states, and new international rules that regulate the issues that remain vague or problematic. One good example of a measure for the cooperative solution of jurisdictional conflict is set in Art.22.5 of the Council of Europe Convention on Cyber-crime according to which when more than one party claims penal jurisdiction, there is an obligation for the parties involved to consult.

The rules can be achieved through the establishment of International Conventions or through the development of International Customary Law. The former alternative may be preferable due to the clarity it brings to issues in a rather rapid time frame, once states agree to a convention. Customary law has traditionally developed more slowly, even though in modern times the concept of instant custom has arisen in some areas such as Space Law. If state practice concerning a certain matter were uniform and consistent, and if almost all

215 <http://www.eff.org/pub/Publications/John_Perry_Barlow/barlow_0296.declaration>

216 www.law.berkeley.edu/journals/ btlj/articles/vol16/geist/geist.pdf

217 http://www.mttlr.org/volfour

states adhered to it, usage would develop into binding international customary law rather quickly. Unfortunately, for the present, that does not seem to be the case where cyber-space is concerned, even though the idea of a world penal law in the context of cyber-crime is blossoming[218].

218 www.itu.int/dms_pub/itu-s/ md/03/wsis/c/S03-WSIS-C-0006!!MSW-E.doc

CHAPTER 23. STANDARDS OF EVIDENCE

The Problem

The proliferation of computers has created a number of problems for law. Many legal rules assume the existence of paper records, of signed records, of original records. The law of evidence traditionally relies on paper records, though of course oral testimony and other kinds of physical objects have always been part of courtrooms also. As more and more activities are carried out by electronic means, it becomes more and more important that the evidence of these activities be available to demonstrate the legal rights that flow from them.

Most electronic records have begun to be admitted in litigations[219]. However, courts struggle with the traditional rules of evidence, with inconsistent results. The common term of "*reliability*" causes confusion between the principles of authentication, best evidence, hearsay and weight in many legal systems.

What is worse, many records managers and their legal advisors have not been confident that modern information systems, especially electronic imaging with the paper originals destroyed, will produce records suitable for use in court.

This uncertainty is beginning to lead to a proliferation of narrowly focused laws by which various government departments across the countries authorize the use of the records from their own computer systems or in dealings between those departments and the part of the public that they regulate. This creates a serious risk of incompatibility in information systems, even within the same jurisdiction. Some provinces have legislated on electronic evidence, but not consistently with each other. As a result, businesses active in more than one jurisdiction may have to keep records differently for use in different jurisdictions.

The law[220] must accommodate the use of technology. It should also be neutral as to technology: people should be able to choose to use paper or any form of technology without prejudice to their legal rights. This means that the way the law will apply to technological choices should be as certain as possible, so those choices can be made for practical reasons.

However, digital evidence differs from tangible evidence in various respects, some of which raise important issues as to how digital evidence is to be authenticated, ascertained to be reliable, or determined to be admissible in criminal or civil proceedings.

---

219 http://www.lawtechjournal.com/articles/2002/03_020625_goodmanbrenner.php

220 Toward a Universal Order of Cyber-Space: Managing Threats from Cyber-crime to Cyber-war World Federation of Scientists, Permanent Monitoring Panel on Information Security August 2003

The problem is how best to incorporate this stream of electronic data into the various processes of legal systems both domestically and in relation to the legal systems of other nations.

Disparities in the international legal environment greatly handicap law enforcement activities and often make it impossible to proceed in investigating cyber-crime cases and in bringing perpetrators to justice. The speed and flexibility of cyber-attacks which can take place in an instant, or which can be spread out over extended periods of time in a low and slow attack scenario that can be very difficult to detect, pose significant legal challenges to the traditional law enforcement environment.

Particularly vexing legal issues include, but are not limited to: intercepting communications, searching and seizing electronic evidence, differing requirements for archiving logs of transactions and traffic generated by computer and communication systems, obtaining information from communication and Internet service providers, and ensuring the validity of cyber-crime evidence across a variety of legal jurisdictions.

Business and legal communities have become well aware that computers can contain evidence of significant, and sometimes overwhelming, importance. Whether it's in the form of files (documents, spreadsheets, images, etc.) or data recovered from erased files, operating-system created files, or slack space (supposedly unused space at the end of a file), electronic evidence can no longer be ignored.

Computers are not the only form of electronic evidence that can be used when evaluating what evidence should be produced or requested in a particular case. A number of other *e-evidence*[221] sources leave trails of data that can protect or damage. Such electronic evidence can conceivably include digital audio, video or photographs, program codes, database records, voice mail, instant messages, or even global positioning system information.

Writings created or electronically exchanged do constitute electronic documents, but the mere existence of a document in electronic format does not necessarily make it electronic evidence.

Some of the requirements [222] which can enable the admission of an electronic document into evidence can be summed up as follows:

- Can the document be properly authenticated in terms of authorship and of the integrity of the document itself?
- How close is the record to its original version? Has its integrity been maintained or are there differences between the record and its original version?

221 http://www.ndu.edu/inss/books/Books_2002/Transforming%20Americas%20Mil%20-%20CTNSP%20-%20Aug%202002/15_ch13.htm

222 Cyber Forensics – New Requirements for our Legal Systems by Joe Anastasi

- Is the document hearsay[223]? Does it meet the tests of reliability and necessity?
- How reliable is the program that created the document?
- How reliable is the program that copied or extracted the document during the discovery process?

At its most basic level, authentication represents the process of making sure that something offered as evidence is truly what its proponent says it is. The authentication of electronic evidence[224] poses a multitude of problems, because by its very insubstantial nature, electronic evidence is subject to alteration, intentional or otherwise, that would be difficult if not impossible to detect, even by an expert.

Due to the transitory nature of information stored on computer systems, there are a number of additional legal obstacles that have to be clarified:

- Computer evidence can be readily, invisibly and undetectable altered or deleted,
- Computer evidence can appear to be copied while in fact it is undergoing alteration,
- Computer evidence is stored in a different format to that when it is printed or displayed, and
- Computer evidence is generally difficult for the layman to understand.

The Existing Texts

EUROPE

Convention on Cyber-crime, 2001

Taking into account the existing Council of Europe conventions on co-operation in the penal field as well as similar treaties which exist between Council of Europe member States and other States and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;

Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

1. Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this Section for the purpose of specific criminal investigations or proceedings.

2. Except as specifically otherwise provided in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 to:

a) the criminal offences established in accordance with articles 2-11 of this Convention;

b) other criminal offences committed by means of a computer system; and

223 www.crimeinstitute.ac.za

224 American Bar Association Section Of Science & Technology Law, Unlocking, Discovering And Using Digital Evidence

c) the collection of evidence in electronic form of a criminal offence.

3. a) Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b) Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system is being operated for the benefit of a closed group of users, and does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 3 – General principles relating to mutual assistance

Article 25 – General principles relating to mutual assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:

a) provision of technical advice;

b) preservation of data pursuant to Articles 29 and 30; and

c) collection of evidence, giving of legal information, and locating of suspects.

2. a) A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b) If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact

shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

Article 46 – Consultations of the Parties

1. The Parties shall, as appropriate, consult periodically with a view to facilitating:

a) the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;

b) the exchange of information on significant legal, policy or technological developments pertaining to cyber- crime and the collection of evidence in electronic form;

In other words the Cyber-crime Convention obligates all signatories to have the ability to decide on cross-border preservation requests. To secure preservation, or in emergencies when immediate international assistance may be required, the international network of 24-hour Points of Contact established by the Council of Europe Convention, the High-tech Crime Subgroup of the G8 countries, and by EU Council of Ministers can provide assistance. Even though they have distinct regulations on each part, in practice the mechanisms merge. This network, which was created in 1997, continues to grow every year. Participating countries have a dedicated computer and crime experts who can be contacted twenty-four hours a day.

The strategy to expedite international cooperation lies in the establishment of a network, intended to handle requests for mutual assistance quickly and efficiently (Art. 35)[225]. Each Party is required to designate a point of contact available 24 hours a day, 7 days a week, to facilitate rapid cooperation in investigating cyber-crimes. The drafters designed the network to help in three main areas: (1) the provision of technical advice, (2) the preservation of data, and (3) the collection of evidence, the supply of legal information, and the locating of suspects. These 24/7 networks are required to communicate rapidly with their counterparts in other Parties, each of whom must ensure that trained and equipped personnel are available to staff the network.

USA

Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, July 2002.

International Issues

Increasingly, electronic evidence necessary to prevent, investigate, or prosecute a crime may be located outside the borders of the United States. This can occur for several reasons. Criminals can use the Internet to commit or facilitate crimes remotely, for example, when foreign hackers steal money from a national bank, or when the kidnappers of a national deliver demands

225 europa.eu.int/information_society/ eeurope/2005

electronically by e-mail for release of their captive. Communications also can be laundered through third countries, such as when a criminal in one location uses the Internet to pass a communication through several locations, before it reaches its intended recipient in a final location, in much the same way as monies can be laundered through banks in different countries in order to hide their source. In addition, provider architecture may route or store communications in the country where the provider is based, regardless of the location of its users.

Searching, seizing, or otherwise obtaining electronic evidence located outside of the United States can raise difficult questions of both law and policy. For example, the Fourth Amendment may apply under certain circumstances, but not under others.

The Loopholes

In order to meet the legal requirements for the production of computer evidence in court, the protocols determine that computer evidence needs to be:

- Admissible. It must conform to certain legal rules before it can be put before a jury;
- Authentic. It must be possible to positively tie evidentiary material to the incident;
- Complete. It must tell the whole story and not just a particular perspective;
- Reliable. There must be nothing about how the evidence was collected and subsequently handled which causes doubt about its authenticity and veracity;
- Believable. It must be readily believable and understandable to members of a jury or judges.

One can already hear the plaintive protests of a party against whom the evidence[226] is offered, alleging that the evidence has been fabricated or at the very least tampered with. So far, courts do not appear to appreciate these hazards. This is troubling since legal professionals are very often ignorant of the implications of technical processes and do not seem to fully appreciate the potential for corruption to the legal process as a result of the improper handling of electronic evidence. The loophole lies in that electronic evidence does not need to attain a very high degree of certainty, because as long as there exists a reasonable likelihood that the exhibit is what the profferer says it is, the standard is met. Once admitted into evidence, any argument about the authenticity or value of the exhibit goes to the weight or the merit which the judges or jury attaches to it in the course of resolving the questions that are the subject of the trial.

226 Getting And Protecting Electronic Information: Discovery Tips, Including Hard Drives, Emails, And Detecting Spoliation Of Electronic Evidence by Karl Bayer and Rob Hargrove

Allegations by one party that the proffered electronic evidence has been altered or otherwise tampered with are common, but are typically met with skepticism on the part of the court. As a practical matter, without specific evidence of alteration or tampering, such an allegation will affect the weight of the evidence rather than its admissibility.

Circumstantial evidence[227] is the primary mechanism for establishing the connection between electronic evidence and its creator. E-mail is perhaps the most common category of electronic message that requires authentication. To be introduced as an evidence one must prove that:

- the message recited matters that only the author would have known. subsequent investigation or formal discovery can confirm that this is truly the case, and tend to establish a connection between the message and the alleged author;
- routing information of the message (such as an IP address) contained in the message header will indicate all of the servers and/or routers that a message has passed through and can be used to identify all of the links in the message chain, including the recipient (telephone records may be required to complete this chain);
- the original message was embedded in a reply to that message.

A witness can authenticate the contents of the website much in the same way as he would a photograph or similar exhibit. When the opposing party wishes to contest the trustworthiness of such evidence, he may do so by examining the totality of the qualities of the website.

As a general rule, an original writing is required to prove the contents of a copy. The rule's purpose is to prevent inaccuracy and fraud when a party attempts to prove the contents of a document. With respect to electronic evidence, if data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an original. The loophole is that an infinite amount of originals can be printed out from one electronic document. Even in the event that such evidence is considered a duplicate it is admissible to the same extent as an original unless there is a genuine question as to the authenticity of the original.

The first task when examining[228] an electronic message, document or record is to see if the process that created that evidence is completely automated, for example, without human intervention in the process. Examples would include audit logs, telephone call records and printouts of electronic access passes used on toll roads. If this is the case, the message cannot be hearsay; only statements or assertions, verbal or non-verbal, can qualify as such. This has created some confusion in the courts, especially since the

227 http://law.richmond.edu/jolt/v10i5/article53.pdf.

228 The Essentials of Computer Discovery by Larry Johnson-Director of Electronic Discovery Services and Joan Feldman

printout of the process may also qualify for and have the look of a business record.

The Suggested Solution

There is a growing sophistication with respect to electronic evidence. Legal technology trade show now routinely feature tracks designated for electronic evidence and computer forensics. The litany of steps involved in correctly applying the law to such evidence during the discovery process and throughout trial can be daunting, both in terms of how to articulate requests for such evidence, and the proper strategy for identifying all potential sources of that evidence. The challenge and responsibility lies in appreciating both the complexities as well as the subtleties involved. Such complexities are demonstrated by the many layers of abstraction that a document may contain, be it actual or metadata[229], while the subtleties are demonstrated the number of places in which a copy of that document may be found, be it on servers, in temporary files or volatile memory. There are simply too many people creating electronic documents; a continual struggle will be waged between those trying to minimize access to internal documents and those trying to access them.

As more and more proprietary information is stored on networked systems, the availability, integrity and confidentiality of this information is increasingly at risk, and the difference between competitive intelligence, economic espionage and information warfare becomes simply a matter of technical degree. Law enforcement agencies are not immune from information warfare and must ensure the integrity and security of their records. Overseas police forces have already been subjected to information warfare attacks that have highlighted the potential risks to evidence and case intelligence.

Evidence collection is probably one of the most challenging issues facing criminal computer prosecution. All computer crimes cause special problems due to the nature of the files themselves. Computer files are easily erased, moved, or tampered with, and that makes using them as evidence very difficult. Largely inexpert investigators find the complex technology and operational difficulties of obtaining computer records as evidence to be a complicated and convoluted subject; and equally inexpert courts find the presentation of such evidence fraught with potential challenges to its verity.

This is already evident in financial investigations: high speed, world wide computer funds transfers are a facet of emerging cyber-payment technologies that add complexity to law enforcement's ability to trace criminal activity and recover illicit proceeds. Additionally, computer hackers use program code to instruct the software they use to erase itself after an illegal transfer of funds has been accomplished, eliminating any evidence of the transfer. The use of such

229 www.4law.co.il/Lea410.htm

programming code makes it almost impossible for law enforcement to track money moved electronically.

The well funded, structured, informed and experienced attacker is likely to go undetected and, therefore, operates with impunity. Part of the reason for this is the absence of a smoking gun in computer investigations. The professional computer attacker leaves no traces: audit records are removed or altered, access times on files are modified; no traces, and therefore no evidence of a crime. Court challenges concerning the integrity and authenticity of electronic evidence have increased noticeably in the past years. This may be the result of persons charged being more computer literate or possessing technical skills; counsel for accused persons having gained computer expertise; more legal precedents having been established; and laws not having kept pace with technological developments.

It will, therefore, be incumbent on law enforcement agencies to devise generally accepted practices, procedures, and principles for the collection and presentation of computer evidence. The failure to develop standards could result in the courts imposing their own rules in an arbitrary and non-uniform manner.

Cyber-space is still in the early stages of its development, but it is already transforming our world[230]. Over the next decade, newer telecommunications, computing and media enabling technologies will affect almost every aspect of our lives. Crime will be no exception. Crime in cyber-space is likely to become more prevalent over the next years. This is because of a lack of general understanding as to the value of security safeguards; a lack of knowledge as to how to cope with the continual emergence of new security holes, the absence of reliable quantitative data to illustrate the nature and extent of crime in cyber-space; the increasing commercialization of cyber-space; and differences in national policies, laws and practices regarding security resulting in difficulties for law enforcement at an international level. It is also possible that cyber-space attacks will result in a blurring of responsibilities between law enforcement, national security and defense interests, necessitating an enhanced level of international liaison and cooperation.

In order to enhance the effectiveness of the future legal regulations, decisions regarding the creation, maintenance and use of documents, and their management systems, must be made in the context of globally harmonized laws and rules of general application. The management of information must comply with applicable laws, regulations and agreements, with generally established professional practices and standards, and with applicable administrative rules and policies.

230 www.aic.gov.au/conferences/internet

CHAPTER 24. TRANS-NATIONAL EXTRADITION

The Problem

Extradition[231] is the formal process by which a criminal suspect held by one government is handed over to another government for trial or, if the suspect has already been trialed and found guilty, to serve his or her sentence.

The consensus in international law is that a state does not have any obligation to surrender an alleged criminal to a foreign state, as the basic principle of sovereignty is that every state has legal authority over the people within its borders. Since there is no such automatic international obligation, and since most countries nevertheless desire the right to demand such criminals of other countries, a web of extradition treaties has evolved. Most countries in the world have signed bilateral extradition treaties with most other countries, but no country in the world has an extradition treaty with all other countries. For example, the United States lacks extradition treaties with over fifty nations at preseent.

An extradition treaty spells out the terms of an extradition. It includes a list of crimes for which a person can be extradited, or else covers them all with descriptions such as any crime for which a prison term could exceed two years. It is usually reciprocal in terms of conditions, but there are exceptions. Generally, an extradition treaty requires that a country seeking extradition be able to show that:

- the relevant crime is serious;
- there exists a *prima facie* case against the individual sought;
- the event in question qualifies as a crime in both countries (the principle of double-criminality);
- the extradited person can reasonably expect a fair trial in the recipient country;
- the likely penalty will be proportionate to the crime.

Extradiction is frequently subjected to other conditions also. Many countries reserve the right to refuse to extradite an individual if, in the government's opinion, they are being sought for a political crime. Many countries, such as Mexico, Canada and most European nations, will not allow extradition to nations with the capital punishment unless they are assured that the death penalty will not subsequently be imposed. Such restrictions are normally clearly spelled out in the extradition treaties that governments have agreed upon. However imposing restrictions on one state national level by another is controversial, because it is often seen as an attempt by foreign nations to interfere in their own sovereign[232] right to manage justice within their own borders.

231 http://conventions.coe.int/Treaty/EN/CadreListeTraites.htm

232 http://www.law.indiana.edu/fclj/pubs/v50/no1/wilske.html

In certain countries, such as France and Germany, the law bars the government from extraditing anyone who is a citizen of the state. This is reflected in the extradition treaties to which such countries are a party. Such restrictions are occasionally controversial in other countries when, for example, a French citizen commits a crime abroad and then returns to his home country to avoid prosecution. The laws of France and Germany do, however, allow for the trying citizens in their home country for serious crimes committed abroad. Those governments will prosecute such a case on the demand of the foreign country in which the crime was allegedly committed.

The usual extradition treaty safeguards relating to double-criminality, the presence of *prima facie* evidence[233], and the possibility of a fair trial have been waived by many European nations for a list of specified offences under the terms of the European Union arrest warrant. The warrant entered into force in eight European Union member-states in January 2004. Defenders of the warrant argue that the usual safeguards are not necessary because every EU nation is committed by treaty, and often by legal and constitutional provisions, to the right to a fair trial, and because every EU member-state is subject to the European Convention on Human Rights.

Issues of international law relating to extradition have proven controversial in cases where a state has abducted and removed an individual from the territory of another state without previously requesting permission, or following normal extradition procedures. Such abductions are usually in violation of the domestic law of the country in which they occur, as infringements of laws forbidding kidnapping. Many also regard abductions as violations of international law, in particular of a prohibition on arbitrary detention.

Where an accused person is resident in a country other than the one in which criminal proceedings[234] are to be taken, it is possible for that person to be extradited to that country to stand trial. Extradition requires not only that an appropriate treaty exist between the two countries concerned, but also that the conduct in question be criminalized in both the referring and receiving country.

Few, if any, countries enforce penal sentences or orders on foreign governments. Even within federal systems, special legislation or constitutional provisions are used to enforce minor penal sanctions such as *on the spot* fines for traffic and parking offenses. The reason for this lies in the assumption, in international law and practice that no nation-state will attempt to exercise its power or public authority within the territory of another, without its express agreement.

---

233 Susan W. Frenner, Joseph J. Schwerha, Transnational Evidence Gathering and Local Prosecution of International Cyber crime, 20 J. Marshall J. Computer & Info. L. 347

234 Jack L. Goldsmith, "The Internet and the Legitimacy of Remote Cross-Border Searches," University of Chicago Law School, October 2001

The power to tax is regarded, like the power to punish, as an exercise of sovereign power. In the absence of the agreement or treaty arrangements, neither the civil nor criminal courts of any country will recognize or enforce the penal or revenue judgments or orders made by courts (or other aspects of the implementation of public policy) of those countries.

Extradition involves both the executive and judicial branches of government and usually takes place under a bilateral treaty that sets out grounds for extradition, although ad hoc extradition is possible. A number of such extradictions have taken place after the events of September 2001. Each country also usually has general extradition legislation, setting out general procedures for, and conditions of, extradition orders. After initial contact between governments, leading to police action, such as the issue and execution of an arrest warrant, the accused must be brought before a court where he or she is. That court must be satisfied of matters set out in the legislation, and the accused has the opportunity to contend that extradition is improper, for example that the crime of which he or she is accused is not an extradition crime within the meaning of any relevant treaties or legislation.

The procedure[235] may be complex and time-consuming, and the authorities of the prosecuting nation may decide that the time and expense are not justified, relative to the returns. It is questionable whether the offences that occur in computer mediated communication networks have yet reached the level of concern that would warrant extradition procedures.

The Existing Texts

EUROPE

Convention on Cyber-crime

Title 2 – Principles relating to extradition

Article 24 – Extradition

1.a) This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

b) Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition, applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.

2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

235 usdoj-crm/mis/mdf

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognize the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that Party.

7.a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Furthermore the Convention provides that, if a party refuses to extradite solely on the basis of the nationality of the person sought or because the requested party deems that it has the jurisdiction over the offense, then upon request of the party that sought extradition, the case will be submitted to local authorities for investigation and prosecution in due course, and final outcome should be reported to the requesting party.

AUSTRALIA

The Australian parliament has enacted the Cyber-crime Act 2001 which came into force on 21 December 2001. This Act inserts a new part into the Commonwealth Criminal Code Act 1995 and largely follows the provisions of the Council of Europe's Convention on Cyber-crime. Unfortunately, this legislation applies only to law enforcement agencies and not to corporate investigators and private sector consultants who deal with the vast majority of Australia's cyber-crime. Although the Convention and the Cyber-crime Act resolve problems to do with copying data from hard drives, obtaining access to encrypted files, and seizing aggregated data, questions still remain concerning the scope of warrants, the ability to intercept e-mails prior to delivery, data not held on the accused's premises, extra-territorial searches, and the scope of mutual assistance orders.

KOREA

Korean Extradition Act Article 4 proclaims the principle of reciprocity. Even though no extradition treaty exists, the Act is applicable if it is guaranteed that any state requesting an extradition would comply with an extradition request of Korea with respect to the same kind of extraditable crime. The Act also limits extradition only to offenses that are punishable for a maximum period of at least one year. Nonetheless, if an extradition treaty or arrangement already exists between Korea and the other state, that treaty or arrangement has priority over the above conditions.

The Loopholes

The federal structure of some nations, such as the United States, can pose particular problems with respect to extraditions. This is because foreign countries do not have official relations with sub-national units such as the individual states composing the US; rather, they have relations with the federal government. This means that the federal government may, in a particular case, certify to a foreign nation that the death penalty will not be sought, and that if it is pronounced it will not be applied, but such a commitment may not be binding on state courts when the matter is one of state jurisdiction. Should an individual state then decide to execute an extradited person, the federal government would be in violation of its commitment to the foreign nation.

Less important problems[236] can arise due to differing qualifications for crimes. For instance, in the United States, transportation across state lines is a prerequisite for certain federal crimes. Such a transportation clause is, understandably, absent from the laws of many countries. Extradition treaties or subsequent diplomatic correspondence often include language providing that such criteria should not be taken into account when checking if the offense is an offense in the country from where extradition should take place.

Most cyber-crime, it is argued, is conventional crime (fraud, drug dealing, money laundering, sexual exploitation of minors), in which cyber-technology happens to be used as the enabling tool. Existing treaties and international arrangements, including those providing for extradition and legal assistance, are potentially applicable in these cases. Securing international agreement on the wording of new cyber-crimes is indeed difficult. Moreover, vast differences exist among states regarding the appropriate regulation of content, the proper scope of transnational investigation, and the bases upon which tracking information and messages should be subject to seizure and scrutiny. Furthermore, great disparity exists among states, even technologically advanced ones, as to the scope of privacy and other rights possessed by individuals under national laws that would either operate to limit an international agreement or be compromised by one.

236 http://web.mit.edu/gtmarx/www/soccont.html

Over the last fifty years in the United Nations, in various European organizations and elsewhere there has been an explosion of instruments dealing with various aspects of international criminal law. At the top of this tree there are the international crimes which include war crimes, crimes against humanity, terrorism, torture, drug offences, crimes against the environment, fraud, corruption and transnational organized crime.

These international crimes can then be divided again into those which are crimes of great enormity, such as war crimes, crimes against humanity and terrorism, and those international crimes which are transnational in execution, such as drug trafficking, fraud, and other types of organized crime.

The one thing they all possess is the need for different forms of international cooperation, such as extradition, mutual assistance, transfer of proceedings, transfer of prisoners and execution of judgments.

Such cooperation permits states to assist each other in the application of their criminal laws. There are however several instruments[237] which develop a supranational perspective on criminal law. They include the International Criminal Court, the international criminal code and some human rights dimensions of international criminal law. So, a large number of international instruments are available.

Below the multinational level again there are a very large number of instruments that operate at a regional level and at a bi-lateral level. A prosecutor with a case that shows the need for enquiries, evidence and people from abroad has to move swiftly if he is to obtain what he needs in time for the trial process. He ought to start from bilateral accords that may exist between his country and the country where the evidence or people are thought to be.

Given that potential for multiple territorial and extraterritorial jurisdictions, resolving the resulting jurisdictional conflicts will inevitably require an agreement between states. It is therefore possible that the effective exercise of an agreed jurisdiction will involve extradition, since the state of physical location of the suspect may not necessarily be the appropriate forum for prosecuting the crime.

Computer crimes[238] do not thus appear to raise any specific difficulties, provided the requirements of the extradition law and/or treaty are met. The most important issues are the requirement, again, of double criminality, namely, that.the impugned conduct would be an offence punishable under the law of both the requesting and the requested State, and the fulfilling of any other conditions that would include computer crime within the category of extraditable offences. This could be accomplished either by setting sanctions for the open formula, for example, a maximum punishment of a certain

237 http://www.acpr.gov.au/publications2.asp?Report_ID=103

238www.cbs.curtin.edu.au/Workingpapers/other/Utilisation%20of%20Internet%20Anonymity%20by%20Cyber%20Criminals.doc

number of months, or by including computer crime in the enumerated list of extradition crimes appended to the extradition treaty in question.

Both conditions require careful attention in the computer crime area. The first condition highlights once again the absolute need to legislate the substantive law in each state as consistently as possible, thus avoiding loopholes or conflicting interpretations of the requirements of criminality.

The second condition, the extraditable character of the offence, requires an attentive legislative drafting polic [239] . In particular, offences such as unauthorized access to computers or telecommunications facilities are often characterized as minor offences, and penalty scales may not meet the minimum threshold standards of extraditable crimes. Unfortunately, experience shows that trans-border hacking cases are common, significantly affecting important transnational economic networks. It might be advisable to consider serious penalties, at least in cases where the hacking affects the international relations of the victim, whether the victim is a legal or physical person or a state. Disregarding the use of extradition or other cooperation methods could seriously hinder the efficiency of the cooperative response to this important and disturbing phenomenon.

Other important concerns, not specific to networking but potentially magnified by it, relate to grounds of refusal where the offence for which extradition is requested is, under the law of the requested state, viewed as having been committed in whole or in part within the territory of that state. A second problematic scenario is possible if the invoked ground for jurisdiction is an extraterritorial one but the law of the requested state does not provide such jurisdiction in similar cases. These situations might also create positive or negative conflicts of jurisdiction. The creation of channels of consultation or negotiation on order to solve such conflicts is highly recommended.

The Suggested Solution

How then, can these problems be overcome? The solutions lie in harmonizing laws and procedures globally, improving the technical capabilities of investigators, and finally in sharing information between public and private sector investigators and enhancing international cooperation.

The continuing harmonization of laws and the adoption of international conventions on cyber-crime and transnational and organized crime will make prosecutions easier and will greatly improve mutual assistance and extradition of offenders. This is already starting to occur, with the adoption of the United Nations of the Convention against Transnational Organized Crime in November 2000, and the adoption by the Committee of Ministers of the Council of Europe of the Convention on Cyber-crime in November 2001. These Conventions contain provisions criminalizing certain conduct, as well as

239 www.uncjin.org /8th.pdf

provisions dealing with special investigative techniques, witness and victim protection, cooperation between law enforcement authorities, exchange of information, training and technical assistance, and prevention at the national and international levels.

The traits relevant to extradition are reciprocity and double criminality[240]. Reciprocity rests on the notion that if one nation honors another nation's request for extradition, the requesting nation will do likewise when the situation is reversed. Reciprocity is most often a more critical factor when no treaty exists between the two nations.

Double criminality requires that the offense charged be considered criminal in both the requesting and requested jurisdictions. This sometimes functions as a loophole that allows cyber-criminals to escape from prosecution. Although the majority of nations today criminalize computer crimes, the lack of legal uniformity still causes serious extradition problems. Inconsistencies in the criminalization of particular conduct are likely with crimes such as adult pornography and dangerous speech.

It should be noted that, extradition law has some exceptions, for example, when a crime is interpreted as having a political nature. Even in such cases, it is still applicable if the life of the chief of a nation, or of a large number of citizens, is endangered by the crime.

240 conventions.coe.int/Treaty/EN/Reports/HTML/090-rev.htm - 75k

CHAPTER 25. TELECOMMUNICATIONS REGULATION

The Problem

The regulation of telecommunications systems[241] and services reflects the dynamic interaction of technology, economic forces, institutional settings and constraints, and interest groups. This evolutionary process of change and adaptation has generated two distinct organizational types: state monopolies and private regulated firms.

Despite these different approaches to ownership as well as institutional implementation, each of these two models constitutes a rather unique mode of regulation of the industry.

In the US, regulation was seen as a set of sector-specific rules developed and enforced by dedicated agencies. Despite the fact that regulatory agencies became hybrid organizations, combining legislative, executive, and judicial functions[242], regulation was thus distinguished from national legislation. It was, further, distinguished from more generic rules, such as the Constitution, that apply to all sectors. Regulation was and is perceived the negation of market forces and as an interference in the working of unfettered markets, to be tolerated only if justified in the public interest.

Elsewhere, in the context of state-owned telecommunications monopolies, regulatory functions were generally more dispersed and less transparent. Frequently, the operator of telecommunications services was also entrusted with main regulatory functions, such as the licensing of other service providers or the setting of standards. Prices were usually set by the legislature.

The functions of telecommunications networks could be distinguished into interactive services (telephony) and one-to-many communications (broadcasting). Cable television, satellite communications, and terrestrial wireless communications were fit into this framework, often as hybrids subject to one set of rules or the other, depending on the service provided. Things became more complicated as online services expanded rapidly, and new cable companies emerged offering Internet access services.

The structure of the Internet has led to diverse and largely decentralized governance of its operation. Likewise, most governments have adopted a much less heavy-handed mode of regulation when it comes to Internet than when it comes to traditional telecommunications. However, a variety of concerns have recently led to calls for greater centralization of governance functions, or even for some kind of international, general purpose, Internet governance body. This governance debate has become a central issue in the World Summit on the Information Society (WSIS).

241 Twilight for Traditional Telecom Regulation? Issue #91 October 25, 2004 by Adam Thierer

242 www.vii.org/papers/citi.htm

Regulatory approaches are largely facilities-oriented. Facilities are but one component in the value-added chain of providing services and applications. While applications such as voice mail, e-mail, user groups, are now a permanent presence in cyber-space, it is the new "virtual reality" applications that have created an entirely freash physical experience. They are to a large degree independent of spatial constraints and may thus not fit well into a regulatory model that has a strong spatial and jurisdictional structure.

To manage these challenges it was necessary to differentiate networks, services, and applications, into their constituent parts. Such an approach helps disaggregate regulatory tasks and functions and in fact differentiates telecommunications, broadcasting, and cable.

The Existing Texts

Regulatory reform in the telecommunications service sector has focused on opening monopoly markets[243] to full competition over the last decade. The liberalization of telecommunication markets has required a new set of regulatory principles that can ensure fair competition in the marketplace. As a result, OECD Member countries have changed their regulatory frameworks for the telecommunications sector as liberalization in the telecommunications market was implemented[244]. Consequently, together with the changes in regulatory rules, there have been changes in the role of regulatory institutions in the telecommunications sector.

One of the most visible institutional changes is the establishment of the independent regulator that is separate from interested parties in order to ensure fair competition in the marketplace. In this regard, in line with the liberalization of the telecommunications market, many OECD countries have established sector specific independent regulators that are separate from not only telecommunications operators but also from line-ministries, which have the responsibility for policy making in the sector. However, the responsibility and the degree of independence of the sector specific independent regulators vary across countries. The relationship between the Ministry responsible for telecommunications policy making and the sector specific independent regulator can be influenced by a country's political and legal traditions and the degree of market development. However, experience has shown that more effective regulation can result where there is a certain degree of structural independence allowing the regulator to implement its regulatory mandate without any political intervention.

Another important institutional change is the growing involvement of competition authorities[245] in telecommunications regulation. In spite of the presence of the sector specific regulator (either as a newly established

243 Regulation and Internet Use in Developing Countries

244 http://www.olis.oecd.org/olis/1999doc.nsf/LinkTo/DSTI-ICCP-TISP(99)15-FINAL

245 Terror-Communications Acts By Tim Druckrey

independent regulator or a traditional government body), as competition has developed the role of competition authorities has increased in the telecommunications sector. It has increased through forbearance by the sector specific regulator and/or the abolition of the exemption on applying general competition rules to the telecommunications sector. The growing involvement of the competition authority raises the issue of inconsistent jurisdiction in the sector which may create problems for market participants in making business decisions. In order to reduce business risks due to regulatory uncertainty, Member countries are using various methods to prevent conflict in jurisdiction between regulatory bodies.

Although the introduction of competition has resulted in changes in the role of institutions, convergence in the communications sector, which is driven by the rapid development and implementation of digital technology[246], is also leading governments to consider future institutional changes. Convergence in communications brings into question the existing service-based vertical regulatory system, which almost all Member countries have adopted. In particular, there is increasing demand from the industry to reorganize regulatory institutions in the light of convergence. However, not many institutional changes have been made to take into account convergence between telecommunications and broadcasting.

While most OECD Member countries have made institutional changes with the liberalization of telecommunication markets, the responsibilities and the structure of regulatory bodies[247] have differed significantly among them. These include changes in the role of regulatory institutions, as well as the development and implementation of a number of new regulatory rules such as licensing, interconnection, numbering, pricing, universal service, and rights-of-way.

The process of liberalization has also been linked with efforts to introduce harmonized regulatory principles in countries in order to ensure consistent market entry opportunities for telecommunications operators. For instance, the European Commission issued Harmonization Directives, such as the ONP (Open Network Provision) Framework Directive, Interconnection Directive and Licensing Directive. The WTO agreement on basic telecommunications services set down principles on interconnection, universal service, licensing, and allocation and use of scarce resources.

Despite these efforts to set down the main principles for telecommunications regulation, there has been a wide variation in how countries have structured regulatory institutions and the role they have given them in facilitating the transition of the market from monopoly to competition while protecting users' interests. At the international level, the only reference to

246 www.oecd.org/dataoecd/39/32/21330624.pdf

247 OECD, Working Party On Telecommunication And Information Services Policies, Telecommunications Regulations: Institutional Structures And Responsibilities

the structure of regulatory institutions is the requirement that it should be independent of telecommunication operations. As a result, regulatory institutions have developed somewhat differently in each country with different responsibilities.

Nevertheless, there have been three major trends.

- First, many countries have established sector specific independent regulators that are separate from line-ministries, which have the responsibility for policy making in the sector.
- Second, competition authorities have been given an enhanced role in the communication sector as competition has developed.
- Third, although not as apparent as the other two trends, some countries are beginning to take into consideration the integration of regulatory institutions on telecommunications and broadcasting in the light of convergence between the two communication services.

The performance of a regulatory system largely depends on the regulator's determination to promote competition regardless of the form of the institutional structure. Furthermore, each country's regulatory structure should be understood in the context of its economic, social and political background.

EUROPEAN UNION

Telecommunications Policy

Through a series of directives, the EU has spelled out rules for implementing the principles of competition, interoperability, technology neutrality and universal service in electronic communications, including telecommunications. Taken together, the EU's directives provide a roadmap for telecommunications[248] liberalization.

The regulatory framework was updated by the EU in March 2002. By July 2003, all Member States of the EU had adapted national legislation implementing the new Directives.

The new directives are intended to provide a coherent and flexible approach to the regulation of electronic communication networks and services. The new policy framework takes due account of the convergence of telecommunications, broadcasting and IT sectors and reinforces competition in all market segments. The proposals provide a lighter regulatory touch where markets have become more competitive yet ensure that a minimum of services are available to all users at an affordable price and that the basic rights of consumers are protected. This framework does not cover the content of services delivered over electronic communications networks using electronic communications services, such as broadcasting content, financial services and certain information society services.

The components of the EU electronic communications policy are:

248 http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm

- Framework Directive: A common regulatory framework for electronic communications networks and services, which addresses basic topics including the independence, procedures and transparency of national regulatory authorities, numbering, rights of way, co-location and facility sharing, and standardization.
- Access and Interconnection Directive: The guidance for national regulators on how to ensure interoperability and competition. This harmonizes the way in which Member States regulate access to, and interconnection of, electronic communications networks and associated facilities. The aim is to establish a regulatory framework for the relationships between suppliers of networks and services that will result in sustainable competition, interoperability of electronic communications services and consumer benefits.
- Authorization Directive: The rule that, except with respect to radio frequencies and numbers, the provision of electronic communications networks or services may only be subject to a general authorization. An undertaking may be required to submit a notification, but may not be required to obtain an explicit decision or individual license or any other administrative act by the national regulatory authority before exercising the rights stemming from the authorization. Upon notification, an undertaking may begin activity.
- Universal Service Directive: The aim of this Directive is to ensure the availability throughout the Community of good quality publicly available services through effective competition and choice and to deal with circumstances in which the needs of end-users are not satisfactorily met by the market. It establishes the rights of end-users and the corresponding obligations on service providers. Also it defines the minimum set of services of specified quality to which all end-users have access, at an affordable price.
- Regulation on Unbundled Access to the Local Loop (2000): This gives national regulators detailed guidance on how to give new entrants access to the copper wire local loop of the former monopoly service provider.
- Consolidated Directive on Competition in the market for Communications Services: This enables the competitive provision of a full range of electronic communications services, including broadband multimedia and high-speed Internet.
- Data Protection Directive for the Telecommunications Sector: This addresses the processing of personal data and the protection of privacy in the electronic communications sector.

USA

Telecommunications Act of 1996

To promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies:

Intermediary service provider

1. Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that:

a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or

b) The provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information.

2. Paragraph 1 shall not apply when the recipient of the service is acting under the authority or the control of the provider.

3. This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement, nor does it affect the possibility for Member States of establishing procedures governing the removal or disabling of access to information.

The Loopholes

Telecommunications regulation has evolved[249] from a primarily domestic concern to one of international significance. As liberalization of the telecommunications sector spreads to many countries, it also transforms the international system of telecommunications. In particular, liberalization leads to the emergence of global telecommunications networks, alliances, and carriers, to new types of service providers, and to an end of the traditional notion of telecommunications as a national and territorial sector. The trend of supra-national carriers and ventures in turn leads to pressure on the traditional form of regulation and control of telecommunication networks. This suggests the need to think about the appropriate regulatory structure of the new type of telecommunications firm, supra-national carriers which transcend the traditional national and territorial definition of telecommunications operators.

Traditional regulation and policy was premised on a certain market structure[250]. Change that market structure, and the nature of regulation must change too.

The core of national goals in regulating telecommunications services and providers has been fairly similar from country to country. Such goals include, explicitly or implicitly:

249 How Countries Are Regulating Internet Content, Peng Hwa Ang, Nanyang Technological University

250 www.citi.columbia.edu/elinoam/articles/supra1.htm

- Consumer protection, to guard against monopoly pricing, unreasonable price discrimination, low quality, gatekeeper power, and privacy violations.
- Universal connectivity, to spread service across the geographic and social range.
- Protection of network operators, particularly the assurance of adequate earnings to enable the development of networks
- Promotion of economic growth, technological innovation, and trade.
- Assurance of communications for emergencies, law enforcement, and national security

To accomplish these goals, governments have, in principle, a wide assortment of regulatory tools at their disposal, such as restrictions on ownership control, market structure regulation (for example, entry and exit control, definition of service sectors), company structure regulation; anti-monopoly rules and concentration restrictions, price and profit regulation, conduct regulation (for example, in quality, interconnection, common carriage); investment and service approvals, and representation in trade negotiations.

These traditional tools of government were predicated on a certain industry structure. But that structure is rapidly changing, and telecommunications are being transferred into an internationalized industry.

Internet telecommunication[251] is made possible by applications, such as Internet Phone, which enable telecommunications via the Internet. The dynamics of this development go beyond computer applications. Since the Internet is presently distance-insensitive in respect to price, it is also a means of long distance and international service. This additional level of competition offers substantial opportunities for new entrants, and exerts additional pressures on traditional carriers to meet the challenges of a future which is likely to consist of non-hierarchical, interconnected networks of networks. These pressures will also affect carrier structures, modularization, and organization of the entire company, not to mention pricing, business strategy, and alliances.

This international opening has created, in a few short years, an astonishing number of global telecommunications activities, with no end in sight. A multitude of policy issues is associated with international carriers. Not surprisingly, these issues are too varied to suggest a single approach of international policy and regulation.

Fortunately, most of these problems are not of immediate seriousness. Some immediate issues are those of transition, such as the requirements to reform the international accounting rate system and the resultant need to reform the financing of universal connectivity. Requiring attention are also the problems of asymmetric liberalization, with its potential for discriminatory

251 http://www.bsos.umd.edu/gvpt/lpbr/subpages/reviews/Cranor-Wildman504.htm

extension of market power. The most serious immediate issue is the threat to global free flow of information by the need to conform to the policies of restrictive countries. Similarly, the potential for new types of consumer fraud is disturbing.

There are numerous options[252] for countries to coordinate regulatory policies. Not surprisingly, each option is a trade-off of advantages and disadvantages. The spectrum of options ranges, on the one extreme, from highly centralized arrangements such as international agencies with full autonomous powers, to full reliance on market forces, without any inter-governmental action on the other extreme.

Unilateral adjustments are not necessarily effective, however, in the problems of repelling undesirable activities from other countries or to attract business by becoming a haven country. Similarly, a unilateral strictness of one country can become a de facto international standard if it is too risky or burdensome for users to conform to different rules.

As the matrix of international interrelations becomes steadily more elastic, the overall tendency, in the long term, might lead to reduced regulatory strictness internationally, too. In that sense, liberalization is an expansionary process. It is not so much an ideological choice, but a response to an internal inability to structure a stable equilibrium that serves multiple interests and goals.

When international regulatory solutions are contemplated, it must not be forgotten that the history of international telecommunications agreements and collaborations, from their earliest days, has been one of creating an international alliance to prop up national monopoly arrangements. The goal of most international bodies was to stabilize rather than to open telecommunications markets

Hence, the benefits of any new international collaborative arrangements to dealing with new problems must be weighed against their cost in transaction costs, and in particular against their impact in reducing policy innovation by various countries.

In many cases, the best coordination mechanism would be through market forces and arbitrage rather than through inter-governmental collaboration. This would suggest a liberalization and a reduction in deregulatory asymmetry[253] rather than the creation of regulatory symmetry.

However, market forces by themselves do not deal with all policy[254] problems, such as redistributive goals, negative externalities, law enforcement, and the transition to a competitive system which may require interconnection arrangements. But these are primarily national issues, calling for national responses, with international coordination.

252 http://www.citi.columbia.edu/affiliates/wdrake.htm

253 www.citi.columbia.edu/elinoam/articles

254 The Dogmatic Function Of Law As A Legal Regulation Model For Cyber-Space, Carlos Alberto Rohrmann

There are incentives for one state to be non-uniform. Examples include large countries for which international interaction may be small in relative terms, such as the United States, which can still afford a non-metric system of measurements. At the same time, many other examples for non-conformity in regulation are small countries, or states: Switzerland in banking; Delaware in corporation law; Hong-Kong in tariff duties; Liechtenstein in taxes; Monaco in gambling; Luxembourg in broadcasting. These examples suggest that small countries, especially, have incentives to being nonconforming, probably since the loss in revenue, control, etc. from their own relatively small domestic economies is more than offset by the inflow from the larger countries due to non-conformity. To prevent such non-uniformity, the other states have to impose substantial pressure on these jurisdictions or produce significant compensations.

The Suggested Solution

The past and currently existing regulatory frameworks have two major shortcomings. Firstly, the basic premise that regulation is a substitute of competition and thus can and should be phased out whenever competition is workable, ignores the point, that market processes themselves need an institutional framework to function properly. Markets are socially constructed and the way property rights are assigned, disputes are solved, and business agreements are reached, can make vital differences for the efficiency and distributional characteristics of arrangements. From such a broader perspective it needs to be decided what institutional arrangements need to be in place to evoke the desired sector performance. Functionally, this is equivalent to the design of a set of rules and regulations implemented via legislative tools. Secondly, regulatory theory and practice is rooted in concepts of static economic analysis, modeled on rather strict assumptions of given technology, well-defined market equilibrium, and consumer preferences. In the world of rapidly changing technology and largely unknown consumer behavior, such models may be very misleading and provide little guidance as to the institutional framework required for the most beneficial development of the industry.

As the variety and complexity of uses of telecommunications networks increases, increased attention needs to be based on issues related to the security of transactions, the protection of privacy and copyright, as well as content. Although a vast body of law is applicable also to cyber-communications important issues remain to be solved. For instance, the creation of messages may be critically dependent on solutions to the copyright issues[255]. Likewise, the usage of cyber-networks for electronic commerce between unaffiliated individuals and/or organizations may be critically dependent on a set of

255 www.vii.org/papers/citi.htm

established and proven legal and security provisions. Probably the most contested issue is the question of content regulation. Solutions to this issue are even more dependent on the non-formal institutional infrastructure (values, morale) of a society and issues related to the rather well-understood market structure problems.

The emergence of cyber-networks also raises important equity issues. These are related to but not identical with the universal service question. Electronic information creation, dissemination, storage, is already changing ways of learning, work, and many other aspects of life. Information is commercialized and de-commercialized, and the access conditions to information determine the opportunities of individuals and organizations. There are fundamental tensions and incompatibilities between this public resource character of cyber-networks and their predominantly commercial market organization. Some of these features are modifications of well-known examples of market failure. For instance, there is an inherent trade-off between equity and efficiency in market-driven environments. Market forces will deploy technologies and services to those areas and customers that promise the highest profitability unless explicit measures to counteract these trends are adopted.

The need to significantly upgrade cyber-networks calls for some form of a congestion charge that reflects the capacity expansion costs of the network. Such pricing may be in conflict with the goal of equitable, non-discriminatory access. These issues reach well beyond a narrow interpretation of regulation and need to be solved at a more general societal level.

As cyber-networks and telecommunications carriers increasingly reach beyond national boundaries, many of the issues become international. Significant obstacles exist that restrict a free flow of resources across international borders. Other than the asymmetric market access conditions these include continuing serious ownership regulations[256]. As a result, many carriers and service providers pursue multi-national investment strategies or attempt to achieve global reach via alliances and joint ventures. As ownership restrictions are only poorly justified and thus will probably disappear gradually, a disparity between the powers of national institutions and the international mobility of capital and resources may emerge. In such a scenario, cyber-regulation will more likely be driven by commercial processes than be in control of such processes.

Maximum competition alone will not provide adequate regulation. Future regulation must also include access and pricing issues, and the development of content rules and supporting legal mechanisms.

In order to enhance the role and the effectiveness of future regulations it will be necessary to create a more coherent framework of rules than the one

256 www.unctad.org/en/docs/c1em9d2.pdf

currently represented by the International Telecommunication Union (ITU), the World Trade Organization (WTO), UNESCO, other standard-setting organizations, or regional organizations such as the European Union or ASEAN.

The current model of intergovernmental arrangements may need to be replaced by the delegation of powers to an international agency. The continued fragmented regulatory approach has more disadvantages than advantages.

CHAPTER 26. REGULATORY AND INVESTIGATORY POWERS

The Problem

The Internet, which has turned out to be so central to everyday life, is now being re-discovered as a significant arena for data-mining. The digital environment provides powerful means for the efficient collection of useful information on many aspects of everyday life, such as bank transactions, personal e-mails, private chats, browsed websites, shopping, and contacts.

Consideration of cyber-crime often leads to questions about the standards under which a government is authorized to obtain access[257] to the electronic communications and computer data that may constitute evidence of cyber-crime or other types of crime. Many countries have procedural laws granting the government investigative powers to access information stored in computers. These include judicial orders for the disclosure of stored data and warrants for the immediate search and seizure of computers and computerized data. Many countries also allow real-time interception of communications and traffic data or transactional data that show the origin and destination of communications. A major part of the Council of Europe Convention on Cyber-crime requires governments to adopt laws on search and seizure of computer evidence, disclosure to governments of computerized records of any kind, and electronic interception of communications.

Government seizures or compelled disclosures of data stored in computers, and government interceptions of communications and traffic data, constitute an intrusion on personal privacy, and therefore need to be subject to procedural safeguards.

The OECD requires in its Guidelines for the Security of Information Systems and Networks that, *"Security should be implemented in a manner consistent with the values recognized by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency"*.

UN Resolution 55/63 of December 2000 provides that states, as they adopt laws regarding investigative access to communications and computer data, should protect individual freedoms and privacy. In 1990, the Eighth UN Congress on the Prevention of Crime and the Treatment of Offenders issued a series of recommendations concerning the adoption of investigative procedures, evidentiary rules, forfeiture, and international cooperation in cyber-crime investigations. In 1995, the UN published its Manual on the Prevention and Control of Computer-Related Crime. This extensive document examines a wide range of issues related to crime and technology, including procedural law, substantive criminal law, international cooperation, data protection, security, and privacy.

257 http://www.crime-research.org/library/Model_Code.htm

The right to privacy is recognized as a fundamental human right under the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights, and the American Convention on Human Rights.

Likewise, the Council of Europe Convention on Cyber-crime explicitly requires that interceptions of communications and searches and seizures for stored data be conducted pursuant to the privacy principles set forth in the European Convention on Human Rights. Article 15 of the Cyber-crime Convention provides:

> *1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms…and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.*
>
> *2. Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.*

The Council of Europe Convention on Cyber-crime itself does not spell out specific surveillance procedures that would comply with the European Convention of Human Rights. Those are found instead in the decisions of the European Court of Human Rights, as well as in the surveillance laws of countries like Canada and the United States that have strong traditions of an independent judiciary and protection of privacy. It is important to give close attention to the development of strong standards for government surveillance.in developing and transitional societies especially, where a fully defined set of rules for searches and seizure and surveillance in the offline world may not yet exist.

Under most advanced legal systems, the interception[258] of electronic communications is permissible, but only in accordance with clear standards in the law, requiring justification and prior independent approval. Based upon developing national and international standards, it is possible to identify the following procedural safeguards regulating the interception of communications:

- The standards for interception are transparent, fully and clearly spelled out in legislation available to the public, with sufficient precision to protect against arbitrary application, so that citizens are aware of the

258 http://www.isaInternet.org/noarchive/cyber-crime.html

circumstances and conditions under which public authorities are empowered to carry out such surveillance.

- Approval is obtained in writing from an independent official (preferably a judge), based on a written application giving reasons and setting forth facts justifying the intrusion. Surveillance is limited only to the investigation of specified serious offenses.
- Approval is granted only upon a strong *prima facie* evidence in support of the belief that the target of the search is engaged in criminal conduct.
- Approval is granted only when it is shown that other less intrusive techniques will not suffice.
- Each surveillance order should cover only specifically designated persons or accounts – generalized monitoring is not permitted.
- The rules are technology neutral so that all one-to-one communications are treated identically, whether they involve voice, fax, images or data, wire line or wireless, digital or analog.
- The scope and length of time of the interception are limited, and in no event is the surveillance extended longer than is necessary to obtain the needed evidence.
- The surveillance is conducted in such a way as to reduce the intrusion on privacy to an unavoidable minimum necessary to obtain the needed evidence.
- The enabling legislation describes the use to which seized or intercepted material could be put; information obtained for criminal investigative purposes may not be used for other ends.
- The law specifies procedures for drawing up summary reports for a judge's review and precautions to be taken in order to permit inspection of the recordings by the judge and by the defense.
- In criminal investigations, all those who have been the subject of interception should be notified after the investigation concludes, whether or it results in charges.
- Personal redress is provided for violations of privacy standards.

Many of the same provisions are also applicable to search and seizure orders for computer data.

A number of developed countries have imposed mandates on telephone common carriers, requiring that communications networks be designed to support government surveillance[259]. In addition, some countries have adopted, or are debating, the adoption of laws requiring service providers to retain traffic data on all communications for a specified period of time, a mandate referred to as data retention. These mandates have been very controversial and

259 www.internetpolicy.net/cyber-crime/020800cyber-crime.pdf

have been criticized for threatening the privacy of citizens and the security of networks and for imposing considerable costs on service providers. In 2002 the European Union adopted a directive on privacy in the communications sphere that permits but does not require member countries to adopt data retention requirements.

The Council of Europe Convention on Cyber-crime also recognizes another important privacy right: the legitimacy of anonymous communications. The Explanatory Report makes it clear that the Convention does not impose on service providers any obligation to keep records of their subscribers. Thus, under the Convention, a service provider would not be required to register identity information of users of prepaid cards for telephone service, nor is it obliged to verify the identity of subscribers or to resist the use of pseudonyms by users of it services. In 2003, the Council of Europe issued a Declaration on Freedom of Communication on the Internet in which it expressly stated that, "*In order to…enhance the free expression of information and ideas, member states should respect the will of users not to disclose their identity*". Likewise, the European Commission, in its 2001 Communication on Creating a Safer Information Society, recognized the value of anonymity, stating, "*An increasing variety of authentication mechanisms is required to meet our different needs in the environments in which we interact. In some environments, we may need or wish to remain anonymous*". Also, in its 2001 Communication on Network and Information Security, the Commission stated, *"authentication must also include the possibility for anonymity, as many services do not need to identify the user…"*

The Council of Europe Convention specifically states that the real-time interception laws required under the Convention shall empower competent authorities to compel a service provider, within its existing technical capability, to collect or record, or to co-operate and assist the competent authorities in the collection or recording of, traffic data and communications content.

Strong encryption is an important tool[260] used in securing the Internet. As the European Commission noted in 2001, *"The use of encryption technologies… [is] becoming indispensable, particularly with the growth in wireless access"*. Recognizing this, the general trend in national policies regarding cryptography has been to reduce or eliminate rules limiting the import, export, and use of encryption. In recent years, most developed countries, which previously sought to control encryption, have concluded that, on balance, the general availability of encryption will improve security, not interfere with it. The 1997 OECD Guidelines on Cryptography Policy and a 1998 European Commission report expressed strong support for the unrestricted availability of encryption products and services.

In the late 1990s Canada, Germany, Ireland, and Finland announced national cryptography policies based on the OECD Guidelines, favoring the

260 www.infodev-security.net/handbook/part4-chapter4.shtml

free use of encryption. France, which had long restricted encryption, reversed that policy in January 1999 and announced that encryption could be used in France without restrictions. In December 1997, Belgium amended its 1994 law to eliminate the provision restricting cryptography. The United States, which had sought to limit use of encryption by limiting trade in cryptographic products and services, lifted almost all restrictions on the export of encryption in 2000.

In a growing number of countries, policymakers are concluding that market forces alone are not sufficient to ensure adequate mitigation of cyber-security risks [261]. As the European Commission has noted, action by governments is required because the market offers imperfect incentives for security: market prices do not always accurately reflect the costs and benefits of investment in security; frequently neither providers nor users bear all the consequences of inaction; control over the Internet is dispersed and given the complexity of networks, it may be difficult for users to assess potential dangers.

Regulation, however, carries risks. In some respects, the Internet has flourished as a relatively unregulated communications medium. The global trend over the past two decades has been towards deregulation of communications networks generally. Competition and innovation supports development of new services and technologies, drives down prices, and expands access to communications technology. When technology is rapidly changing, government regulation may hinder the adoption of innovative security solutions. There is widespread recognition that government regulation is likely to be ineffective and even counterproductive.

Instead, one approach is to impose a general requirement to protect security[262]. This approach was taken in Europe, growing out of the concept of privacy protection, where a general duty to protect security is imposed on all entities that collect or process personally identifiable data. Another approach is to focus only on certain economic sectors. The United States for example, in imposing privacy obligations on the financial services and health care industries, also imposed a requirement for companies in those sectors to protect the security of personal data.

Europe has started by imposing security obligations on all entities that collect and process personal information. The EU Data Protection Directive requires that controllers of personal information take appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network. The Directive further states "*such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be*

261 A Regulatory Web: Free Speech and the Global Information Infrastructure by Viktor Mayer-Schönberger and Teree E. Foster

262 http://www.privacy.gov.au/news/speeches/sp34note.doc

processed". Canada takes a similar approach, requiring in general terms under its Personal Information Protection and Electronic Documents Act that private sector companies take security measures to protect personal information they hold.

Finding common instruments and adopting cooperative solutions are of that concern for all countries with Internet access. However, criminal or illegal use of the Internet does not affect all on-line countries in the same way. The United States and the EU, along with Japan and other industrialized countries, just cannot ignore the problem. Over 95% of Internet traffic is produced and goes through OECD countries, with the United States, and the European Union being the main producers of that OECD traffic.

The most difficult obstacle to overcome when investigating the cyber-world is the lack of reliable data and evidence. The main cause of this is that measuring Internet features is hard. Measuring off-line illegal activities is equally difficult.

The Existing Texts

UNITED NATIONS

The UN was perhaps the first international body to recognize the importance of addressing cyber-crime. In December 2000 and January 2002, the UN General Assembly adopted Resolutions 55/63 and 56/121 on Combating the Criminal Misuse of Information Technologies. Resolution 55/63 declares that states should review their laws to eliminate safe havens for those who carry out cyber-crime. Resolution 55/63 recommends, inter alia, that states take appropriate measures to prevent the criminal misuse of information technologies, international cooperation in investigation and enforcement efforts, and the preservation and timely sharing of electronic data and evidence. Resolution 55/63 also recommends educating law enforcement authorities and the general public on cyber-crime issues.

USA

Following the unfortunate events of September 2001 the US has become more active in the digital informational environment, acknowledging its growing significance and identifying its potential importance as a new battle zone. Several aspects of the information environment were identified as relevant in this exercise: First, the Internet, as a major communication pipeline, was perceived as an arena that requires surveillance for preventing future hostile actions. Second, the Internet as a relatively open distribution mechanism, allows the distribution of propaganda by terrorist groups, recruitment of new supporters, collection of donations, and so forth.

Less than two weeks after the September 2001 attacks on New York and Washington DC, the bill Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, was passed by both Houses and signed into law. The

Act amends no less than 15 other acts, and addresses a wide range of issues which enhance the powers of the intelligence services to gather information, process and share it, while lessening judicial oversight.

UNITED KINGDOM

In 2000 the British Parliament approved the Regulation of Investigatory Powers Act 2000 (RIPA). While the Act prohibits interception without lawful authority, authorizes interception without a warrant in certain situations, lists the circumstances in which a warrant can be issued, and regulates in great detail the relevant procedures. The Act also imposes some duties on telecommunications services, a term which includes Internet service providers. The Act was an attempt to achieve several goals: expanding law enforcement's ability to gather information in the digital environment; complying with the requirements of the Human Rights Act 1998 that interference with the right to privacy is allowed only if *"in accordance with the law, and is necessary in a democratic society in the interests of national security…; and responding to European law"*. It also reflects a fundamental switch away from the reactive policing of incidents to the proactive policing and managing of risks. In this sense, RIPA was an early appreciation that the digital environment was an arena of terrorist activity.

The United Kingdom undertook an omnibus legislation, responding to the new realization of the changing methods used by terrorists. Like the USA PATRIOT Act, the Anti-Terrorism, Crime and Security Act 2001, amends several other statutes, only some of which relate to the digital environment. In fact, a law review editorial noted that the Act brings a host of disparate measures, some of which are only distantly related to the security concerns which prompted it. It is fair to say that the 2001 Act strengthens the focus on the digital environment as a potential arena for terrorist activity, and makes explicit the earlier realization of this threat, as embodied in RIPA.

EUROPE

The Council of Europe[263], initiated a legal inquiry into this matter as early as 1989, an initiative which resulted in the 2001 Convention on Cyber-crime. The Convention was adopted by the Committee of Ministers of the Council and opened for signature in November 2001. The Convention does not directly address issues of cyber-terror as distinct from cyber-crime. Although it was drafted before September 2001 (but adopted shortly thereafter), the concepts it reflects, are in line with the post-September 2001 legislation in the United States and the United Kingdom. The Convention's goals are, harmonizing domestic criminal substantive law, providing domestic criminal procedural law to enable investigations and prosecutions of cyber-crimes, and setting an effective international cooperation network. It requires members to adopt legislation to outlaw various computer-related activities, including offences related to child pornography, and infringement of copyrights; it

263 http://www.gilc.org/privacy/coe-letter-1200.html

imposes liability on aiding and abetting, mandates certain procedural rules, and establishes a framework for international cooperation.

The Loopholes

Data retention requirements are far more intrusive than technological capability requirements, as they impose a costly burden on the ISPs. They have a direct effect on the privacy of users, and they turn the ISPs into a long arm of law enforcement authorities.

One kind of data retention requirement refers only to the traffic data. Traffic data refers to the identity of the sender and the addressee of the communications, to the means of communications and to communication that is logically associated with it. In other words, traffic data might include information such as who sent an email to whom, from which IP address and which geographical location, via which ISP, etc.

A legal framework[264], which allows an ISP to prevent interceptions by government officials, simply by inviting such an investigation, could be dangerous. Arguably an ISP, as any other owner, should be capable of protecting property against trespass, by inviting assistance from law enforcement agent. Such a right would equate their legal situation to that of owners of real property who defend their property against burglars. Yet, such authority opens up a back-door for government interception beyond the reach of judicial review. In fact, this type of regulation demonstrates the potential risk in authorizing ISPs to disclose users' information. This regulation creates a convergence of ISPs property and commercial interests, and governmental national security tasks. Notwithstanding their potential value as powerful information junctions, ISPs have their own legitimate commercial interests. Subscriber information is a valuable commercial asset and providers could benefit from data mining and data retention.

The state's duty to provide national security does not mean that the use of any tools to achieve this goal is legitimate. To the contrary: this duty should be checked over and over again, and be balanced against other interests and rights. The State is subject to the Constitution, and therefore the duty derives indirectly from the State's role as a guardian of human rights and the well-being of its citizens. In other words, the duty of the State to provide national security is dependent on the rights of its citizens.

The cyber-world is experiencing a remarkable paradox[265]. On the one hand, digital communications makes anonymity possible, but on the other hand, anyone using virtual communication still leaves a large number of digital trails behind. It is easy to trace these trails and compare them with all sorts of other registers, allowing for the compilation of detailed individual profiles that can cover a considerable part of an individual's life. As a consequence, the life

264 The Limits In Open Code: Regulatory Standards And The Future Of The Internet By Lawrence Lessig
265 http://www.windowatch.com/2002/may/privacy8_5.html

of the modern citizen is becoming increasingly transparent, rather than increasingly anonymous.

Any regime for the indiscriminate retention of personal data is hazardous. The state should be fulfilling its role to uphold the rights of individuals, as technologies become more invasive, and as laws become increasingly reluctant to protect individual rights. Data retention is an invasive and illegal practice with illusory benefits.

The retention of personal data resulting from communications, or of traffic data, is necessarily an invasive act. With the progress of technology, this data is well beyond being simple logs of whom we have called and when we called them. Traffic data can now be used to create a map of human associations and more importantly, a map of human activity and intention.

The claims that the retention of this information is necessary for investigations are not entirely accurate. The security gained from retention may be illusory. It is possible, indeed likely, that traffic data that is associated to one individual may actually be linked to activity undertaken by another, or by a process that is unrelated to the activities of the first user. The linking of one individual to a set of actions through checking logs is a tenuous link at best. We may be attributing actions and intentions to innocent individuals instead.

The European Convention on Human Rights protects the right to private life. The indiscriminate collection of traffic data offends a core principle of the rule of law: that citizens should have notice of the circumstances in which the State may conduct surveillance, so that they can regulate their behavior to avoid unwanted intrusions. It is often claimed that traffic data retention will combat terrorism and officials[266] argue with fervor that retention is a key technique in the struggle for global security. Many laws were then passed in response to terrorism, only for legislators to be shocked to discover that data retention has little to do with investigating terrorism, and is more commonly used for common investigations and surveillance. The perceived security gains may be illusory as retention introduces many additional risks. Innocent individuals may be surveilled, with intimate details of their lives becoming available to any and all agencies of governments.

The indiscriminate retention of traffic data gives rise to a number of challenges. Technologically, the practice of retention is invasive, as it involves indiscriminately collecting and retaining information of a highly personal nature. This is no longer just a log of telephone calls made and received; it the registering of all things that are read, received, sought, in places over time with varying people, all to be used for some unforeseen later analysis. This information can be used to interpret and map human relationships, understand and extrapolate upon human intention, and track every movement of an individual throughout his daily life.

266 http://www.infodev-security.Internet/handbook/part4-chapter4.shtml

The retention of traffic data by communications providers would also greatly enhance the risk that personal information could be stolen and exploited by third parties. Stored traffic data would present an attractive target for malicious hackers, who would be able to access multiple personal details about individuals. As the information would be stored, malicious hackers would be able to sort through stolen data at their leisure, rather than trying to intercept valuable personal details in real time, as at present. Mandatory data retention laws would thus make the job of the cyber-criminal considerably easier.

Concerns[267] about the misuse of sensitive personal information could undermine public confidence in electronic communications systems. An extensive requirement on communications providers to retain traffic data would give all users of electronic services reason to fear that stored data relating to their personal lives might be improperly accessed. A loss of public confidence could, in particular, retard the role of the Internet as a channel of social intercourse and a vehicle for electronic commerce.

The Suggested Solution

In respect of national security, as in respect of other purposes, there has to be a reasonable and genuine link between the aim invoked and the measures undertaken.

In the light of the above, the following recommendations, which are not exhaustive, are suggested for a future law:

- A clear definition of "content data" and its differentiation from "traffic data".
- Traffic data collection might be invasive and we must advocate for sufficient uniform constraint prior to collection.
- Civil liberty protections must be strengthened and invasive techniques used only in cases of serious crimes.
- "Proportionality" must be defined uniformly at the international level.
- The current approach of allowing exceptions and reservations by individual countries fails to set mutually agreed limits to privacy intrusions that will be within the scope of a treaty.

267 Seizing Power In The Information Environment: The Comeback Of The State By Michael D. Birnhack* and Niva Elkin-Koren

CHAPTER 27. DISPUTE RESOLUTION

The Problem

The Internet has already become the commercial backbone of the world economy. As it increases in importance for the national and international economy, its smooth, trouble free operation will be seen as essential to commercial and national interests.

A number of interpersonal, family, community or business disputes could arise in cyber-space in much the same way as they do in physical space. The new types of disputes that arise specifically from new technologies include:

- domain names (there are dispute resolution processes established through the Internet Corporation for Assigned Names and Numbers (ICANN);
- complaints in relation to privacy and security of on-line communications infrastructure complaints and disputes, especially in relation to telecommunications carriers;
- performance and project disputes;
- disputes over trademarks and copyright;
- dispute arising over the circulation of information, or illegal or inappropriate content, over the Internet;
- e-commerce disputes, including those between businesses (B2B), between businesses and consumers (B2C), and between consumers and consumers (C2C);
- workplace conflicts arising out of changes in employment, personnel and work practices, generated by new technology.

The question of what court or tribunal may resolve a particular controversy often arises with respect to conflicts in real space. Efforts to answer it have generated several venerable and formidable bodies of legal doctrine: personal jurisdiction, subject-matter jurisdiction; venue; and the collection of rules and policies collected under the umbrella of alternative dispute resolution.

The same composite question arises frequently in cyber-space also. Firstly, the plaintiff and the defendant in a cyber-space[268] dispute often reside in different countries. Indeed, the defendant's only contact with the jurisdiction in which the plaintiff is inclined to bring suit is likely to consist of having made his or her website available to computer users there. Under such circumstances, the question arises of whether the defendant is amenable to suit in the jurisdiction congenial to the plaintiff. Secondly, speed is often especially important in resolving Internet-related controversies. The glacial pace of most court proceedings is ill suited to such controversies, creating unusually strong

268 A Legal Technical Framework for the Online Resolution of Domain Name Disputes by Christopher Gibson, Jim Fullton

incentives for the identification or creation of alternative forums. Thirdly, many cyber-space disputes raise novel issues of substantive law and of technology, issues that frequently perplex courts of general jurisdiction.

Once a tribunal has been selected, the next question is: what body of substantive law should be use to resolve the controversy. The laws in force in different countries pertaining to the Internet vary considerably. Thus, the choice-of-law becomes important. In the United States, the doctrine that determines which substantive law should be applied is known as *conflict of laws*[269] In other countries it is more likely to be called private international law.

Resolving the substantive nature of a party's dispute is a matter traditionally addressed by national judicial systems. While resolution by courts may have worked under more traditional business models, the Internet, which has essentially eliminated the borders among the countries of the world, poses new challenges. Given the small value of the transaction and the non-enforceability of foreign judgments, judicial proceedings may not be an effective means of resolving a consumer complaint.

Disputes arise because of perceived differences in interests. If there is an interaction between two or more people or companies, and one believes that his or her interests are not identical to those of the other, there will be a dispute. The best way to prevent disputes from arising is to make sure that each party knows what the other party wants, and to capture in clear, unambiguous writing any agreements between the parties. Increasing each party's knowledge about the other decreases the chance of a dispute arising because of a possible misunderstanding. Similarly, relying on business practices that are universally used in a certain industry or region will reduce the number of disputes. Disputes can easily arise when the parties do not know each other well, when they are engaging in new forms of business, or when they come from different cultures.

Alternative Dispute Resolution [270] (ADR) was originally developed to bypass the deficiencies (whether perceived or inherent) found in many traditional judicial systems around the world. Such deficiencies include the inefficiency of these systems, the high costs involved and the procedural complexity underlying the use of these systems. ADR has been used for years to assist in resolving traditional disputes not involving cyber-space. While ADR encompasses a whole range of different dispute resolution methods, the most popular forms are arbitration[271], mediation, negotiation and conciliation. These methods are generally perceived as being able to: (a) reduce the costs and time spent; (b) simplify the processes; and (c) do away with the endless motions and procedural wrangling that characterize the traditional litigation system in most countries.

---

269 cyber.law.harvard.edu

270 Dispute Resolution in Cyber-Space: What It Is. Ethan Katsh, Larry Lessig, David Post, Eugene Volokh

271 Arbitration as a Dispute Resolution Mechanism for the Domain Name System by Chandru Ganesh

Many governments have today recognized that ADR is a potent force, not in replacing the national court systems, but in assisting or complementing them by dealing with disputes which may not be appropriately or effectively dealt with by the courts. Through ADR, cyber-space litigants are able to sidestep many of the difficulties which would surface where resolutions of such disputes are sought in the traditional forums and where obsolete conflicts of rules would inevitably be applied.

Some differences between the most common techniques of dispute resolution of litigation, arbitration, mediation, and negotiation are as follows:

- Litigation: Involves lawyers, the adversary process, formal and public trials before a judge, and, typically, one party ending as the winner and the other as the loser.
- Arbitration: Does not use courts. The parties to the dispute pick one or more arbitrators and agree to abide by the arbitrator's ruling. Lawyers may or may not be involved, proceedings may be private, and the end result can be win/lose or a compromise.
- Mediation: A neutral third person is selected by the parties but the mediator does not make any rulings or decisions. Rather the mediator helps the parties to come to an agreement themselves by meeting with them, both individually and together. The mediator identifies the interests and concerns of the parties, and helps them find areas of agreement. The participation of lawyers is less likely, and any agreement they reach will always involve compromise. No settlement occurs unless both parties agree to it. What this means is that both parties will walk away from a mediation with some measure of satisfaction.
- Negotiation: No neutral third person is used to assist the parties in reaching an agreement. The parties do so themselves.

ADR, or alternative dispute resolution, generally focuses on arbitration and mediation, processes using neutral third parties to settle the dispute out of court[272]. ADR has enjoyed extraordinary growth during the last years. It has been perceived as a less costly approach than litigation and also as a method that allows more flexibility in designing solutions, that is less formal and less reliant on lawyers, and that is private and confidential.

There are cases, such as civil rights cases, where litigation might be the most appropriate method to use even if it is costly and time consuming. Litigation might be preferable to other methods in those cases where it is important for proceedings to be public and for a standard of behavior to be established.

In other cases, however, the parties may have had a relationship before the conflict and might possibly wish to have a relationship in the future. Mediation,

272 www.privatedisputeresolutionservices.com/ publications.html

more than litigation, might reduce the hostility that exists between the parties and enhance the possibilities for a workable future relationship.

Online Dispute Resolution (ODR)[273] is a branch of dispute resolution which uses technology to facilitate the resolution of disputes between parties. It primarily involves negotiation, mediation or arbitration, or a combination of all three. In this respect it is often seen as being the online equivalent of Alternative Dispute Resolution (ADR). However, ODR can also augment these traditional means of resolving disputes by applying innovative techniques and online technologies to the process.

In practice it is difficult to provide a self-contained definition of ODR, and given the pace of change it may not even be possible to do so. The use of technology usually involves the use of Internet-based communications technology at some stage, but ODR does not necessarily involve purely online processes – further, many could be replicated offline using pen and paper, or could be achieved using computers without Internet connections.

International attempts to provide a foundation for lasting, global peace have also focused on arbitration. Two examples of this are the Permanent Court of Arbitration, which resulted from international meetings conducted between 1899 and 1907 in The Hague, and the development of the League of Nations in 1918 which employed arbitration as one mechanism of dispute resolution.

Outside the political arena[274], arbitration and mediation have been used by businesses world wide to settle their commercial disputes. In Europe, businesses of differing national origin have frequently submitted their controversies to arbitration. In the United States, arbitration and mediation are often used to settle labor disputes arising from conflicting interpretations of existing employment contracts, construction disputes, and shareholder disputes concerning the valuation of stock in closely held corporations, to name but a few examples. The submission of a commercial dispute to mediation and/or arbitration may be done voluntarily or at the prompting of a governmental agency.

The Existing Texts

UNITED STATES

In the United States, the establishment of personal jurisdiction by a court over a defendant requires some statutory provision which must empower the court in question to exercise jurisdiction over the defendant. State statutes typically indicate that any of the following will be sufficient:

- the defendant was present in the state when served with process;
- the defendant lives in the state;

273 www.economicexpert.com/a/Dispute:resolution.htm

274 Dispute Resolution in Cyber-Space by Devashish Bharuka and William Fisher

- the defendant is incorporated in the state;
- the defendant consented to jurisdiction, for example, by filing suit in the state or by agreeing to a forum-selection clause in a contract;
- the defendant committed acts that justify the exercise of long-arm jurisdiction.

EUROPEAN UNION

Several Conventions govern the circumstances in which the exercise of jurisdiction would be proper. The central principle of the Lugano Convention on Jurisdiction and the Enforcement of Judgments in Civil and Commercial Matters is that the power of a state to assert jurisdiction over a person domiciled therein will be decided upon according to the internal law of the state itself. Several exceptions to this principle have been enumerated. For example, in contractual relationships, a person may be sued in the courts of the country where the obligation should be performed. In the case of involvement of a branch, agency or other establishment, the courts of the place where such branch, etc. is situated, have jurisdiction to adjudicate the matter. In consumer disputes, the complainant is entitled to bring proceedings against a supplier of goods or services or a creditor in the state where the consumer is domiciled. Finally, an entrepreneur can only bring proceedings against a consumer in the country where the consumer is domiciled. The Romano Convention on the Law Applicable to Contractual Obligations deals with the choice-of-law issues. Parties are free to choose the law applicable to a whole contract or to parts of a contract. In the absence of any valid agreement regarding choice-of-law, the applicable law shall be that of the country most closely connected to the agreement. Here too, consumers are given special protection. A consumer right under the law of his domicile cannot be overridden by a contractual choice-of-law provision if

- the execution of the contract was preceded by specific invitations addressed to the consumer or by advertising directed towards the consumer; or
- the seller or its agents received the order in the country of the consumer.

When these conventions are applied to Internet-related disputes, the physical domicile of entrepreneurs will still be the determining factor when deciding which courts are competent courts and which is the applicable law.

Also important in the EU context is the country-of-destination rule, which entitles a consumer to bring suit in his own domicile whenever the defendant has been pursuing business activities in the consumer domicile or directing commercial activities towards that state.

Alternative Dispute Resolution Directive 2000/31/EC of the European Parliament on certain legal aspects of information society services, in particular

electronic commerce, in the Internal Market Directive on Electronic Commerce.

Article 17 - Out-of-court dispute settlement

1. Member States shall ensure that, in the event of disagreement between an information society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means.

2. Member States shall encourage bodies responsible for the out-of-court settlement of, in particular, consumer disputes to operate in a way which provides adequate procedural guarantees for the parties concerned.

3. Member States shall encourage bodies responsible for out-of-court dispute settlement to inform the Commission of the significant decisions they take regarding information society services and to transmit any other information on the practices, usages or customs relating to electronic commerce.

Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data

Chapter II – Basic principles for data protection Article 10 – Sanctions and remedies: A contractual dispute over software copyright infringement may be settled through mediation. The parties may apply to the arbitration organ for arbitration of a contractual dispute over software copyright in accordance with the arbitration clause in the contract or a written arbitration agreement subsequently concluded. Where the parties have not inserted an arbitration clause in the contract, nor have they subsequently concluded a written arbitration agreement, either of the parties may directly institute proceedings in the People's Court.

CHINA

Alternative Dispute Resolution

Regulations on Computer Software Protection,

Chapter IV Legal Liabilities

Article 31: A contractual dispute over software copyright infringement may be settled through mediation. The parties may apply to the arbitration organ for arbitration of a contractual dispute over software copyright in accordance with the arbitration clause in the contract or a written arbitration agreement subsequently concluded. Where the parties have not inserted an arbitration clause in the contract, nor have they subsequently concluded a written arbitration agreement, either of the parties may directly institute proceedings in the People's Court.

INTERNATIONAL BODIES

A few examples of international bodies that provide international arbitration are:

- The International Court of Justice of the United Nations (ICJ).
- The Permanent Court of Arbitration (PCA).
- The World Trade Organization: Dispute Settlement Processes.
- The International Centre for the Settlement of Investment Disputes of the World Bank (ICSID).

- The United Nations Compensation Commission (UNCC).
- The European Court of Human Rights
- The Central American Court of Justice (CACJ)
- The International Prize Court (IPC)
- The Court of Arbitral Justice (CAJ).

The Loopholes

Accessibility and acceptability will influence whether a new process, such as on-line ADR[275], is accepted in the first place. In addition, the actual and perceived equity of outcomes for parties once they use the service will also influence the choice of this vehicle.

Information technology may neutralize some sources of power by removing some of the dynamic associated with face to face communication, and may empower certain disputants by enhancing their communications capacity. Other forms of power imbalance may however emerge. The style of on-line communication may be more suited to some groups. The cost of on-line communication may lead to time pressures that work against some groups. Those with greater computer literacy and keyboard skills are clearly better able to use the medium to their advantage. Those relatively unfamiliar with the technology may be more easily manipulated into agreement by the other party or by the ADR practitioner.

As parties may access an on-line ADR service anywhere in the world, the neutrality of the forum may become an issue. In the global environment national courts may not be considered wholly independent; ADR bodies[276] from a particular country may similarly be tainted. In a face to face meeting, an ADR practitioner may be able to build trust to overcome this perception. In on-line communication, this may be more difficult, especially if the practitioner is seen as having a possible alignment with the local party.

Impacts are uneven[277] where one party is available for a face to face meeting with the ADR practitioner, and the other is available only via e-mail, telephone or video hook up. While the face to face party may be in a better position than the remote party to communicate with the practitioner, the remote party can more effectively mask feelings, delay responses or manipulate the environment. There is also a risk that the practitioner may overcompensate for the apparently disadvantaged party.

Each mode of communication has advantages and disadvantages. For example: face to face communication provides the fullest degree of interpersonal communication. However, it is not always feasible, and some

275 Dispute Resolution In Cyber-Space: Demand For New Forms Of Adr, Henry H. Perritt, Jr.

276 Experimental Study on Alternate Dispute Resolution (ADR) Eigo Yoshioka, Research Director Consumer Protection Working Group, ECOM

277 Going Private: Technology, Due Process, and Internet Dispute Resolution by Elizabeth G. Thornburg

interpersonal dynamics, for example physical intimidation, may also work against effective resolution.

On-line[278] text communication is quick, accessible, and cheap. It allows for large amounts of text based information to be transmitted, searched and modified. It enables the exchange of large volumes of written information. While e-mail requires typing skills, the act of writing may actually assist parties to reflect on their positions.

E-mail is far quicker and more convenient than conventional forms of written communication. The speed of exchange can be determined largely by the parties, and multiple exchanges, which would take months through an exchange of letters, can be compressed in time.

Telephone communication is almost ubiquitous, is relatively cheap and enables greater human interaction than text. However, it excludes body language.

Video conferencing provides an approximation to face to face interaction. However, images are two-dimensional, and, as eye contact is via a fixed camera, some information gained from face-to-face eye contact is lost. Lagging can create delays in responses and lead to a perception of hesitancy[279]. Physical movement may be constrained by camera angles and bandwidth constraints. Video conferencing also fails to convey other sensory data.

One-way communication may be a stilted and constrained but prevents interruption. Two-way communication is more natural and provides immediate feedback. It allows interruptions, which may have negative or positive impacts.

Asynchronous communication, such as e-mail, voice mail and video streaming, is not dependent on parties being available at the same time. This is a major advantage where parties are in different international time zones. At the same time it leads to a reflective response, which could enable parties to alter or adjust what they would communicate in a face-to-face situation. Asynchronous communication, however, gives parties the space to consider proposals and offers without the pressure of immediate acceptance. By contrast, the immediacy of synchronous communication may lead to greater spontaneity, more pressure and greater risk of words and actions that may be regretted later.

Some information is lost in all forms of current telecommunications technologies, and this loss may have an impact on some of the intangible aspects of human relationships. For example, it may be difficult to create trust. Conversely, the loss of such information may be useful where interpersonal dynamics are destructive, for example, a history of physical intimidation or enmeshed conflict.

Rapidly decreasing costs, increasing competition and increased capacity in many relevant technologies prevent firm cost comparisons. ADR service

278 http://www.disputes.Internet/

279 www.nadrac.gov.au/adr/ DisputeResolutionInformationTechnology.htm

providers[280] may need to shop around for the best deal and regularly revisit their estimates. Information technology may also require new models for charging fees for funding ADR services.

The costs of a face-to-face meeting include the cost of a physical venue, travel costs and time lost in travel. Costs to consider in on-line communication include line rental, software and equipment costs. With on-line communication, costs depend largely on the bandwidth required. E-mail and telephone communication are relatively cheap and accessible, do not require extensive physical facilities, but limit interaction. Low bandwidth videoconferencing is reasonably affordable and accessible, but may suffer from poor picture quality. Other issues to consider in estimating costs are:

- Technology may lead to a duplication of required resources, such as where information and records need to be provided in both electronic form and hard copy.
- New methods require a period of adjustment. Initial increased inefficiency may be expected while people adjust to change.
- Considerable training, marketing, consumer education and capacity building may be required before on-line ADR is accepted.
- The use of technology may shift costs. For example, a technologically supported ADR session, such as a videoconference, may reduce travel costs for the parties, but increase overheads for the ADR service provider.

While some disputes may be better suited for litigation because the precedents are important, the benefits and the shortcomings of the techniques of Alternative Dispute Resolution (ADR) are as follows:

Benefits of Mediation

- Allows parties to come to a mutually agreeable solution.
- Facilitates communication between the parties.
- Results can be tailored to meet their situation.
- Less expensive than litigation or arbitration.
- Fees are split between the parties unless otherwise agreed.
- Protects the confidentiality of the parties.
- Faster than litigation processes.

Drawbacks of Mediation

- If entered into after onset of litigation, one party may simply be using it as another discovery tool.

Benefits of Arbitration

- Less expensive than litigation because it is (a) faster than litigation, and (b) the parties may agree to limit the range of monetary awards.
- Less formal procedures.

280 Overview of Dispute Resolution ,Richard Hill

- Reaches a final result on a specific issue which is holding up an overall settlement.

Drawbacks to Arbitration

- Contractually limited selection of arbitration
- Non-neutral or conflicted arbitrator
- No value as legal precedent as results are not made public
- Lack of deterrence

The Suggested Solution

In the light of the above the following are some of the recommendations that can be suggested:

- The arbitration of disputes might be made compulsory within the telecommunications industry ;
- Provisions should be made for a party to appeal to a panel of arbitrators if not satisfied with the award of a single arbitrator ;
- The mechanism must be easy for both the consumer and business to utilize and expeditious to ensure the viability of the mechanism;
- Fees must be appropriate so that they do not dissuade consumers or businesses from utilizing the mechanism while, at the same time, ensuring its financial viability;
- The mechanism must ensure that the parties to a dispute have a meaningful opportunity to present their case and to participate in the process of the resolution of the dispute;
- To be truly effective in the borderless online marketplace, any mechanism must be international in nature, ensuring effective resolution of disputes between parties in distant locations.

CHAPTER 28. TREATY SECRETARIAT

The Problem

In international law, a treaty[281] is a formal agreement between sovereign states or organizations of states. The term is ordinarily confined to important formal agreements, while less formal international accords are called conventions, acts, declarations, or protocols.

A treaty ordinarily deals with the rights and duties of nations, but treaties may also grant specific rights to private individuals. Although treaties deal with a great variety of subjects, they are commonly classified under a few heads. Political treaties deal with alliances, war, cessions of territory, and rectification of boundaries. Commercial treaties may govern fisheries, navigation, tariffs, and monetary exchange. Legal treaties concern extradition of criminals, patent and copyright protection, and the like.

Treaties are designed to regularize the intercourse between nations, and, as such, they are the source of most international law. In some countries treaties are a part of the law of the land and are binding upon all persons.

Treaties have existed ever since states came into existence. Records survive of Mesopotamian treaties dating before 3000 B.C. The Greeks and the Romans had elaborate ceremonials to emphasize the sanctity of treaties, and many current treaty practices like *pacta sunt servanda* and *rebus sic stantibus* have classical antecedents.

A treaty is negotiated by duly accredited representatives of the executive branch of the government. The preliminaries are not usually open to the public, but the record of all negotiations is usually preserved for use in case the treaty provisions require subsequent interpretation.

Technical experts draft the text, which the government representatives then sign. The treaty is next ratified by the signatory states in accordance with their constitutional procedures, and it comes into effect when these ratifications are formally exchanged.

Members of the United Nations[282] are required to register their treaties with that organization. A treaty that has not been registered in this fashion may not be invoked before a UN agency. If treaties between UN members conflict with their obligations under the Charter of the United Nations, the Charter takes precedence.

The interpretation of treaties, like that of all legal documents, may present great difficulties. There is no tribunal with compulsory and final jurisdiction to interpret a treaty. Parties may, however, voluntarily submit a dispute to the International Court of Justice or the Permanent Court of Arbitration at The Hague.

281 www.un.org/law/ilc/texts/trbtstat.htm

282 http://untreaty.un.org/English/TreatyHandbook/chapter5.htm

Treaties may end in various ways. Most provide for a date of expiry, or a time at which notice to terminate must be given. Treaties terminate if one of the signatory states becomes politically extinct, or in the case of political treaties, if the parties are at war with one another. A treaty may be terminated by mutual consent, and breach of a treaty by one party entitles the other to abrogate it.

As treaties are agreements between governments in the first place, individual citizens cannot directly appeal to them. Nevertheless, they can be involved in a few ways. Once an international treaty is concluded and ratified it become effective, and imposes a liability on the government to observe the agreement.

Every treaty has its own secretariat[283], which monitors the observance with its clauses and rules, and in this quality organizes regular inter-governmental meetings of the parties to the agreement. More and more treaties now include a provision that civil society or NGO's may be admitted as observers to these meetings, as there is a growing tendency among governments to involve their citizens in the implementation of international agreements. Like other laws and policy documents, all information about the data of the periodical meetings is normally freely accessible to the public.

The Existing Texts

The regulations regarding the Secretariat of a treaty vary greatly about its functions and purposes. This is because parties are free to decide the mandate of the secretariat and its working procedures.

From the point of view of the Law of Cyber-Space, the United Nations Convention on the Law of the Sea sets a very relevant example of functions of the Secretariat. It lays down a comprehensive regime of law and order in the world's oceans and high seas, establishing rules governing all the uses of their resources. It enshrines the notion that all problems of ocean space are closely interrelated and need to be addressed as a whole.

The Convention was opened for signature in December 1982. This marked the culmination of more than 14 years of work involving participation by more than 150 countries representing all regions of the world, and all legal and political systems. At the time of its adoption, the Convention embodied in one single instrument the traditional rules for the uses of the oceans, while at the same time introducing new legal concepts and regimes to deal with new concerns. The Convention also provided the framework for further development of specific areas of the Law of the Sea.

283 http://www.rec.org/REC/Publications/PPManual/FeeBased/ch15.html

LAW OF THE SEA – SUB-SECTION D. THE SECRETARIAT

Article166: The Secretariat

1. The Secretariat of the Authority shall comprise a Secretary-General and such staff as the Authority may require.

2. The Secretary-General shall be elected for four years by the Assembly from among the candidates proposed by the Council and may be re-elected.

3. The Secretary-General shall be the chief administrative officer of the Authority, and shall act in that capacity in all meetings of the Assembly, of the Council and of any subsidiary organ, and shall perform such other administrative functions as are entrusted to the Secretary-General by these organs.

4. The Secretary-General shall make an annual report to the Assembly on the work of the Authority.

Article167: The staff of the Authority

1. The staff of the Authority shall consist of such qualified scientific and technical and other personnel as may be required to fulfill the administrative functions of the Authority.

2. The paramount consideration in the recruitment and employment of the staff and in the determination of their conditions of service shall be the necessity of securing the highest standards of efficiency, competence and integrity. Subject to this consideration, due regard shall be paid to the importance of recruiting the staff on as wide a geographical basis as possible.

3. The staff shall be appointed by the Secretary-General. The terms and conditions on which they shall be appointed, remunerated and dismissed shall be in accordance with the rules, regulations and procedures of the Authority.

Article168: International character of the Secretariat

1. In the performance of their duties the Secretary-General and the staff shall not seek or receive instructions from any government or from any other source external to the Authority. They shall refrain from any action which might reflect on their position as international officials responsible only to the Authority. Each State Party undertakes to respect the exclusively international character of the responsibilities of the Secretary-General and the staff and not to seek to influence them in the discharge of their responsibilities. Any violation of responsibilities by a staff member shall be submitted to the appropriate administrative tribunal as provided in the rules, regulations and procedures of the Authority.

2. The Secretary-General and the staff shall have no financial interest in any activity relating to exploration and exploitation in the Area. Subject to their responsibilities to the Authority, they shall not disclose, even after the termination of their functions, any industrial secret, proprietary data which are transferred to the Authority in accordance with Annex III, article 14, or any other confidential information coming to their knowledge by reason of their employment with the Authority.

3. Violations of the obligations of a staff member of the Authority set forth in paragraph 2 shall, on the request of a State Party affected by such violation, or a natural or juridical person, sponsored by a State Party as provided in article 153,

paragraph 2(b), and affected by such violation, be submitted by the Authority against the staff member concerned to a tribunal designated by the rules, regulations and procedures of the Authority. The Party affected shall have the right to take part in the proceedings. If the tribunal so recommends, the Secretary-General shall dismiss the staff member concerned.

4. The rules, regulations and procedures of the Authority shall contain such provisions as are necessary to implement this article.

The Secretariat of the Law of the Sea is thus headed by the Secretary-General. It is organized into four functional units:

- Office of the Secretary-General
- Office of Administration and Management
- Office of Legal Affairs
- Office of Resources and Environmental Monitoring

The main functions of the Secretariat include:

- Preparing and submitting draft texts, reports and other documents, analysis, research findings, policy suggestions and recommendations:
- Providing secretariat services to the Assembly, the Council, the Legal and Technical Commission and the Finance Committee; providing information and advice to the bureau of those organs and bodies and to delegations; and assisting in planning the work of the sessions, in the conduct of the proceedings and in drafting reports;
- Providing meeting services (including interpretation, translation, document reproduction services and press releases);
- Producing publications, information bulletins and analytical studies;
- Organizing and servicing expert group meetings, seminars and workshops;
- Disseminating information on the activities and decisions of the Authority;
- Programme planning and allocating resources for the effective, economic and efficient performance of the services and functions of the Secretariat.

The functions of the Office of the Secretary-General are to:

- Assist the Secretary-General in the implementation of general policy;
- Supervise and co-ordinate the work of the Secretariat;
- Be responsible for the external relations of the Authority;
- Be responsible for protocol matters, liaison and representation, organization of official ceremonies and similar functions;
- Maintain up-to-date lists of Permanent Representatives and other persons accredited to the Authority, issue official identification passes and notify the host government of arrivals and departures of persons accredited to the Authority;

- Co-ordinate with the office responsible for conference services of the United Nations on the conference servicing requirements of the Authority;
- Ensure the timely preparation, translation, printing and distribution of official documentation.

Administration and management staff provide general administrative and management support to the Secretariat. Functions include financial management and control, preparation of proposed budgets, assessment of contributions of member states, recruitment of staff and contractors, procurement of goods and services, personnel management and security.

The Office of Legal Affairs (OLA) provides legal advice relating to the substantive work of the Authority as well as secretariat services to the organs of the Authority, including preparation of official documentation and liaison with the Department of Conference Services of the United Nations.

One of the primary responsibilities of OLA is to work with the seven contractors for exploration for poly-metallic nodules to ensure that contractual obligations are met and that necessary reports are submitted in a timely manner to the Legal and Technical Commission. OLA assists the Legal and Technical Commission in its consideration of such reports.

Some of the other specific tasks that OLA is responsible for include the following:

- Providing general legal services to the Secretariat and advising the Secretary-General as required on legal matters, including providing legal advice on financial, personnel and pension matters, the interpretation of the Financial Regulations and Rules, Staff Regulations and Rules, and the Rules and Regulations of the United Nations Joint Staff Pension Fund;
- Advising on matters relating to the privileges and immunities of the Authority and its staff, the permanent representatives to the Authority and the representatives of members of the Authority;
- Preparing agreements and memoranda on cooperation with other international organizations, and draft relationship agreements between the Authority and other national or international institutions;
- Maintaining appropriate relations on legal matters between the Authority and the Office of Legal Affairs of the United Nations Secretariat and its Division for Ocean Affairs and the Law of the Sea, the Commission on the Limits of the Continental Shelf and the International Tribunal for the Law of the Sea;

The Office of Resources and Environmental Monitoring is headed by the Deputy to the Secretary-General and Interim Director-General of the Enterprise, and includes both the scientific and the technical arm of the Authority's Secretariat.

The functions of OREM include the following:

- Provision of secretariat services to the organs of the Authority;
- Provision of economic, technical and scientific inputs in the preparation of and monitoring compliance with the rules, regulations and procedures for the conduct of activities in the Area;
- Implementation of the decisions of the Preparatory Commission relating to the registered pioneer investors and their certifying States;
- Development and maintenance of the information technology facilities of the Authority to support the basic data processing needs of the Authority and to provide for a central data repository;
- Development and maintenance of a central data repository of resources of the international seabed area;
- Supporting the environmental monitoring programme of the Authority;
- Promotion and encouragement of the conduct of marine scientific research with respect to activities in the Area;
- Managing the production and distribution of the Authority's publications, including dissemination of public information on the work of the Authority and the decisions of its governing bodies.
- Monitoring trends and developments relating to deep seabed mining activities including world metal market conditions; and assessment of the available data relating to prospecting and exploration for poly-metallic nodules of the Area, including areas reserved for the Authority.

As part of the OREM program of activities, its newly established Central Data Repository (CDR) is continuously being updated as data comes to hand. The objective of the CDR is to collect and centralize al public and private data and information on marine mineral resources and their associated biodiversity and make them available to interested parties on the Internet.

Another ongoing activity for OREM is the cataloguing of books and publications available from the Authority's Library. The library manages the Authority's specialized collection of reference and research materials on matters relating to the Law of the Sea and deep seabed mining and serves the needs of member states, permanent missions and researchers interested in the law of the sea and ocean affairs.

These regulations of the Law of the Sea may serve as a relevant guide for a future global treaty on the Law of Cyber-Space.

The Loopholes

The establishment of every treaty secretariat is contingent on the particular needs of a specific treaty. Signatory parties will always have to ensure that the

secretariat of the treaty will perform all the specific functions and responsibilities that are required.

The Suggested Solution

In the light of the above the following recommendations[284] are suggested:

The Secretariat functions may include:

- the arrangements for sessions of the Conference of the Parties, the Executive Board, and subsidiary bodies and all ancillary services as may be required;
- the provision of support to Members, on request, in the compilation and communication of information required in accordance with the provisions of the Treaty;
- the preparation of reports on its activities under the Treaty;
- the transmission of reports received by it pursuant to the Treaty;
- the assessment of technological developments relevant to the Treaty;
- the monitoring and review of the trends and developments in the area of Information Technology;
- the collection and evaluation of information and data relating to the area of the Treaty;
- the facilitation of the compilation and dissemination of data necessary to accomplish the objectives of the Treaty;
- the necessary coordination with the competent international and regional intergovernmental organizations and other bodies;
- the receiving and transmitting of official communications;
- the administration of agreed arrangements for monitoring, control and surveillance, and for the provision of scientific advice;
- the study of managerial policy options for the administration at different stages of its operations;
- the entry into such administrative or contractual arrangements as may be required for the effective discharge of its functions;
- the publishing of the decisions arrived at by the relavant bodies under the Treaty;
- the treasury, personnel and other administrative functions;
- the performance of all other secretariat functions specified by the Treaty and by any of its protocols.

Once the negotiations on a Law of Cyber-Space are completed, and agreement is reached on harmonized legislation, the next step would lie in the

284 Toward a Universal Order of Cyber-Space: Managing Threats from Cyber-crime to Cyber-war- Report and Recommendations, World Federation of Scientists, Permanent Monitoring Panel on Information Security. August 2003.http:www.//it is-ev.de/infosecur.

need to make the component laws enforceable and to increase public awareness about them. If the United Nations is given the task of setting up the secretariat, it will then be for the contracting parties to agree on the degree of powers that will be given to such a United Nations body for enforcement and coordination. This will be a highly technical function, and would require a very intimate relationship between an inter-governmental body like the United Nations, and the other two stake-holders, namely, the private sector and civil society. No Law of Cyber-Space can be durable or enforceable without the full cooperation between all these three stake-holders, a cooperation that is based on mutual trust and respect, and a common commitment to the objectives of harmonized legislation.

BIBLIOGRAPHY

1. Charter of the United Nations available at www.un.org/aboutun/charter.

2. U.N. Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States (Non-Intervention Treaty) available at www.un.org/documents.

3. The Universal Declaration of Human Rights available at www.un.org/Overview/rights.html.

4. International Covenant on Civil and Political Rights available atwww.unhchr.ch/html/menu3/b/a_ccpr.htm.

5. European Convention on Human Rights available at www.hri.org/docs/ECHR50.html.

6. American Convention on Human Rights available at www.hrcr.org/docs/American_Convention/oashr.html

7. United Nations of the Convention against Transnational Organized Crime available at www.unodc.org/unodc/en/crime_cicp_convention.html

8. United Nations Convention on the Law of the Sea available at www.un.org/Depts/los/.

9. Trade-Related Aspects of Intellectual Property Rights-World Trade Organization agreements available at www.wto.org/english/docs_e/legal_e/ursum_e.htm#eAgreement.

10. UNCITRAL Model Law on Electronic Commerce available at www.uncitral.org/uncitral/en/uncitral_texts/ electronic_commerce/.

11. UNCITRAL Legal Guide On Electronic Funds Transfers available at www.uncitral.org/uncitral/ en/publications/publications.html.

12. OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data available at www.oecd.org/document/.

13. WTO Declaration on Electronic Commerce available at www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm.

14. Treaties of Rome of 1957 available at www.unizar.es/euroconstitucion/Treaties/Treaty_Rome.htm.

15. 1980 Rome Convention on the law applicable to contractual obligations available at www.europa.eu.int/comm/justice_home/fsj/civil/applicable_law/fsj_civil_applicable_law_en.htm.

16. Draft Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters available at www.europa.eu.int/comm/justice_home/unit/civil/audition10_01/index_en.htm.

17. The Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters available at www.curia.eu.int/common/recdoc/convention/en/c-textes/brux-idx.htm.

18. Berne Convention available at www.wipo.org/clea/docs/en/wo/wo001en.htm

19. Universal Copyright Convention available at www.unesco.org/culture/laws/copyright/html_eng/page1.shtml.

20. Patent Cooperation Treaty available at www.wipo.org/ipdl/en/.

21. Eurasian Patent Convention available at www.eapo.org/eng/documents/konvenci.html.

22. Paris Convention available at www.wipo.org/treaties/en/ip/paris/.

23. European Patent Convention available at www.european-patent-office.org/legal/epc/.

24. EUROPE -Convention on Cyber-crime available at conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

25. The Council of Europe's 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data available at conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.

26. Safe Harbor Agreement USA –European Union available at www.export.gov/safeharbor/sh_documents.html.

27. USA Digital Millennium Copyright Act available at www.usdoj.gov/criminal/cyber-crime/iplaws.htm.

28. USA Can-Spam Act available at www.ftc.gov/bcp/conline/pubs/buspubs/canspam.htm.

29. USA Patriot Act available at www.epic.org/privacy/terrorism/hr3162.html.

30. APEC Privacy Principles available at www.apec.org/apec/enewsletter/march_vol2/onlinenewse.html.

31. Australian Cyber-crime Act 2001 available at www.efa.org.au/Issues/Security.

32. Toward a Universal Order of Cyber-Space: Managing Threats from Cyber-crime to Cyber-war, Report & Recommendations, World Federation of Scientists Permanent Monitoring Panel on Information Security, August 2003, available at www.itu.int/dms_pub/itu-s/ md/03/wsis/c/S03-WSIS-C-0006!!PDF-E.pdf