15th BILETA Conference: "ELECTRONIC DATASETS AND ACCESS TO LEGAL INFORMATION".

Friday 14th April 2000.
University of Warwick, Coventry, England.

Regulating Cyberspace

Flora Teichner
Multimedia University
Malacca, West Malaysia.

Abstract: The internet was created in the 60´s. Criminals have used every possible means to commit crimes. Today they have exploited computer technology to suit their criminal purposes. Some of the areas that the paper will consider are the developments of cyberlaws and the problems involved in regulating this space. Finally, this paper will highlight the importance of global interactions as computer crime is a global problem rather than a domestic problem.

Keywords: computer crime, legislation, internet, controls, problems, global responses.

Introduction

The Internet originated in 1969 as an experimental project of the Advanced Research Project Agency (ARPA) which was an American research project, later called ARPANET. The network only linked computers and computer networks owned by limited bodies. It evolved beyond its original research objectives and eventually it was called the "Net." In the last 30 years, it has enhanced civilization in numerous ways but it has also created immense opportunities to commit crimes. This weakness was recognised by [1]Wasik:

..... the sheer diversity of behaviour within the context of computer misuse, where the computer may figure at one moment as the instrument of crime, and at the next as the target for crime, and given the importance of non-economic motives in some forms of computer misuse, such as the unauthorised access of computer systems purely for intellectual challenge and some cases of computer sabotage, makes any monolithic explanation of this phenomenon quite implausible.

One of the causes which allow the Net to be misused in so many ways is its malleability. This was said by [2]Yochait Benkler.

'Information in the Net is more malleable than any information in any form previously known to us, except oral communication. It is mutable, and can be represented in writing, sound and colour. It also allows us to communicate over distances and at speeds of which we could only dream not too many years ago. This new mode of communication, its malleability, transmissibility, networking capacity, and processability affect our lives in many and sometimes suprising ways..... It requires that we find new legal solutions for new social questions...[and] it also affects how we think about legal problems and their potential solutions in the first place. A major implication of electronic

communications is the breakdown of traditional legal categories intended to address technological distinctions that are no longer pertinent. ...

When bodies linked to the Net go online, they communicate in a space called "cyberspace". [3]It was reported recently that there are 196 million Internet users world wide. [4]An alternative forecast based on data collected by the Computer Emergency Response Team, (funded by the federal government of the United States) which is an Internet security group headquartered at Carnegie-Mellon University, gives the number of Internet users between 200 million and 2 billion by the year 2000. It is horrendous to even think that 1% of this population go unpunished because there are no proper means of governing these communications.

The objectives of this paper are as follows:

* To highlight some of the computer crimes that have taken place in cyberspace;

* To determine the various methods of regulating these crimes;

* The discuss some of problems encountered in regulating these crimes;

* To signify the importance of global co-operation to fight these crimes.

[5]In a dramatic demonstration of the Internet´s vulnerabilities, electronic vandals disrupted some of the Web´s most popular sites using dozens of powerful computers to spew out a crippling flood of false data. Internet sites under unprecedented attack included those of eBay, Amazon and CNN. All assaults were similar to one that overwhelmed Yaahoo! a day earlier. All these assaults are called computer crimes or computer-related crimes and they cover a very wide spectrum of crimes.[6]To call all these activities as computer crime may not be appropriate, but a narrower definition is simply not untenable. The [7]United States Department of Justice (DOJ) has defined "computer crimes" as "any violation of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution." Hacking is a common type of computer misuse. And it has taken place long before laws were implemented to prevent this type of misuse. In the late 80´s cybercriminals in the United Kingdom were found not guilty since there were no laws to convict them[8], or the application of [9]existing laws were not tailored to capture these offenders. The defendants in [10]*R v Gold and Schifreen* hacked because hacking was their hobby. They managed to obtain the password given to British Telecom engineers. This allowed them to use the e-mail facilities and have access to several databases. They left a message in the e-mail box of the Duke of Edinburgh. They were eventually tracked down. The prosecution brought a charge under s 1 of the Forgery and Counterfeiting Act 1981 which states as follows:

*'A person is guilty of forgery if he makes a false **instrument** with the intention that he or another shall use it to induce somebody to accept it as genuine and by reason of so accepting it do or not do some act to his own or any other person´s prejudice.'*

The were convicted, but appealed to the Court of Appeal. Their conviction was quashed on two grounds. Firstly, because the Court was of the opinion that material such as discs and tapes whereby the material is stored by electronic means did not fall within the definition of an 'instrument' found under s8 of the Act. The Court was of the view that the definition of an instrument under s8 covered physical objects and not electric impulses which appeared only for a few seconds. Secondly, the Court found no element of forgery since the password was a genuine password. The defendants were only not entitled to use this password.

[11121314]

This case was a turning point, whereby the English courts had to come to terms that

their pre-existing laws did not accommodate nor reflect the changes that were brought by computer technology. Computer criminals could be any persons. It could be a youthf

Crimes on the Net

Crimes on the Net have taken place long before appropriate legislation were implemented. This study will highlight some of the crimes that have taken in some parts of the world. [15] http://www.wired.com/news/news/pentagon[/]The Israeli Prime Minister Benjamin Nethanyahu reportedly has praised the skills of a fourteen year old Ehud Tenebaum, also known as "Analyzer", who is accused of breaking into hundreds of the United States government computer systems. [16] Mathew Bevan 23 who is the son of a Fraud Squad broke into the United States Air Force computers. The estimated damage was about 300,000 pounds sterling. Bevan walked out free, since the prosecutors thought it would not serve the interest of the public as the case will be expensive. Furthermore, the trial may lasts for about 3 months and witnesses must be brought from the United States to give evidence against the hacker. In [17]*US v Morris*, the defendant had planted a "worm" which almost crashed the NASA and the United States Defense Systems. He was convicted under the Computer Fraud and Abuse Act 1986 but only received a probationary sentence. [18]The Defense Information Systems Agency intentionally "attacked" 38,000 Department of Defense (DOD) computer merely to test DOD´s security system, and out of the 24,7000 penetrations, only 4% were detected by the system administrators. Of which only 27% were eventually reported. [19] Pentagon reported that from 250,000 attacks on its computers in 1995 and 65% of these attempts were computer network entry. In an incident in 1994, hackers were able to access the Rome Laboratory´s System . Through this system the hackers gained access to NASA´s Goddard Space Flight Center, Wright Patterson Air Force Base and other government facilities and stole vital DOD information including air tasking orders.

Similar intrusions have taken place in the United Kingdom. [20]It has been reported that since 1993, assaults on computer systems of banks and other financial institutions are possible with the help of the latest generation military weapons which target communications systems. This has resulted in great losses. This is because the organisations involved pay ransom money. In another incident that involved the famous Dr. Lewis Popp who sent many people disks through the mail. It was supposed to contain certain vital information about the Aids virus. The disks contained the said information but in addition it also contained 'Trojan horse' whereby it would have been activated if the computer was used more than 100 times. The case never come before the court because the mental state of the accused was said to be impaired. [21]Christopher Pile also known as the 'Black Baron' created two pernicious viruses called the 'Quegg' and 'Pathogen' He pleaded guilty to five charges of gaining unauthorised access to computers, five of making unauthorised modifications and one of inciting others to spread the viruses that he had written. Many British companies suffered losses. Estimated losses were up to 5,000,000 pounds and about 480 staff hours to check for the virus in more than a million files. [22] In *R v Cropp*, the defendant visited the premises of his ex-employer, a wholesaler. Cropp showed interest in an item, picked up a machine and the salesperson was called away while entering the details in the storeroom computer. The defendant knowing the system, punched in a discount of 70%. His employer thus paid an amount of 204.60 pounds plus VAT instead of 710.96 pounds plus VAT. He was the first person charged under the Computer Misuse Act 1990 but due to judicial interpretation he was acquitted. The trial judge held that a computer could only be hacked if one computer accessed another. [23]*Bedworth* is a clear example of the ineffectiveness of the Act. The defendant pleaded not guilty to the charges because the defence raised his computer addiction as a defence to negate the necessary criminal intent. `Computer tendency syndrome' was accepted as a defence although the trial judge highlighted to the jury that addiction, obsession and dependence were not criminal defences. Considering what [24]Charlesworth in the case of [25]*Lawrence* said , it is not likely that the courts will consider addiction in mitigation. It must be said that *Lawrence* was case where burglary was committed to satisfy the addiction. Thus it may not be proper to draw a similarity between the two cases. However, it is an indication to show the general approach the

courts take towards such criminal defences . [26]Bulgaria was said to have the highest rate of computer virus production per capita of any country, yet the government is unable to track the criminals down. The Internet is relatively a new area in Asia, however it is gaining its popularity in the region. In Singapore, [27]http://singapor[e]statistics released by the Ministry of Home Affairs show that from 1993 to 1995, only three cases reached court. All involved mobile phone cloning. In 1996, the numbers increased to 14 cases of computer crime two crackers (malicious hackers), four counts of unauthorized access of computer materials, six mobile phone cloning cases and two cases of pager cloning. The next year, 1997, the number jumped to 39, including 20 counts of unauthorized usage of computer services and five cases of unauthorized usage of computer material. It is also becoming rampant in other Asian countries. [28]It was reported that computer hackers broke into yet another Japanese government website on Saturday the 29th January 2000, it being the seventh in less than a week. They left behind a message in Chinese language and a picture of the Japanese flag. The Tokyo Metropolitan Police did not immediately confirm the report. All these attacks indicate that no country is free from predators who wish to test and exploit the vulnerabilities of the Net. There are three ways how an offender may use a computer to commit crimes. This depends on the role of the computer in the commission of the crime.

* First, the computer may be the "object" of a crime. An example of this will be the theft of a computerises services.

* Second the computer may be the "subject" of a crime. Implanting [29]"viruses," [30]"Trojan horses," and [31]"logic bombs" are instances where the computer is considered as the "subject" of a crime.

* Finally the computer is used as an "instrument" to commit crimes, [32]whereby the computer may be used to collect credit card information to make fraudulent purchases.

The United States and Cyberspace

* Governments around the world have realised that cyberspace should not be used as a paradise for criminals. Is cyberspace a no-man´s-land whereby rules and laws have no impact? This notion is false, for cyberspace laws or better known as cyberlaws are now constantly being implemented by countries around the world as an attempt to solve problems raised by this innovation. This space is distinct form other spaces, for this global communication creates a new dimension to human activities. The nature of the Net, the availability of information being stored in digital form and the possibility of working with people over great distances raise new issues that have to be dealt with. The discrepancies can only be resolved if there are proper means that reflect the changes the electronic age has brought. Legislatures around the world are at different stages of drafting and implementing cyber laws. This study will look at the governance or regulation of cyberspace from three angles.

* First, the laws that are implemented.

* Second, efforts of government agencies in curbing these crimes.

* Third, the need of security measures. The United States of America created the Net almost 30 years ago. It was the first country that had laws to stop computer criminals.

* There are at least forty different federal statutes that computer criminals could be prosecuted. Computer Fraud and Abuse Act 1986 is one of the main legislation that has been successful in prosecuting cybercriminals. The first law to fight computer crime was Counterfeit Access Device and Computer Fraud and Abuse Act 1984[33]. The Act made it an offence to knowingly access a computer system without express or implied authorisation. This included unauthorised modifications, destruction or disclosure of information found on the computer system. However the

Act was still said to be ambiguous and narrowly drafted. These defects were said to be rectified by Computer Fraud and Abuse Act 1986.[34] This Act was the result of several years of research and discussion with legislators. The Act was aimed at overcoming obstacles in obtaining evidence from victims of computer crimes. Banks and financial corporations especially were not prepared in giving evidence that may expose the vulnerabilities of their organisations. [35]The Congress played a vital role in expanding the scope of the computer crime law. This Act was further amended by the Computer Abuse Amendments Act 1994. However, the National Information Infrastructure Protection Act 1996 contains the most recent amendments to the Counterfeit Access Device and Computer Fraud and Abuse Act. Listed below are some of the changes that the Act has made.

* The 1994 Act eliminated the "federal interest computer" language of the former Act and replaced it with broader expression. The effect was that the Act applied to anyone who "through means of a computer used interstate commerce or communications, knowingly causes the transmission of a program, information, code or command to a computer or computer systems..." With this section, private owned computer systems used in interstate commerce or communications are protected just as federal interest computers[36]. The Act only covered crimes involving computers located in more than one state. The 1996 Act has substituted "federal interest computers" with "protected computers." " Protected Computers" include those computers used in interstate commerce or communications. This means the present statute protects any computer attached to Net, even if these computers which are involved are all from the same state.

* The Act also solved problems that existed by revising s 1030(a) (5). The 1986 Act, required that damage be done by those without authorised access. This meant that insiders who with intent, damaged computers that they had authority to access were not covered under the Act. The 1994 Act rectified this defect by removing the trespass requirement and inserting an intent or recklessness element, thus leaving negligent trespassers uncovered. Under the current law however, it is a crime to cause damage intentionally to protected computer by "transmission of a program, information, code or command, " regardless of authorisation to access the computer. It is also a crime to cause damage, may it be recklessly or negligently or otherwise, if protected computer was intentionally accessed without authorisation. Therefore company insiders and authorised users are legally responsible for only intentional damage and unauthorised users such as crackers implanting viruses are responsible even if the transmission was only [37]negligent or [38]reckless.

* Under the 1994 Act, defenses were available because of ambiguities in the legal language, such as defenses based on intent, value of access or implied authorisation. Under s1030 (5) (c) now it is clear that only an intent to access is needed to be established an not an intent to cause damage. [39] *US V Morris* the defendant was charged under the 1986 Act. He argued that under s 1030 (a) (5), the prosecution must prove that he not only intended an unathourised access to a federal interest computer but also that he intended to prevent others´ access. He went on further, by saying that he had possessed authorised access to the computer and therefore he should not be found guilty under the Act. He justified himself by saying that the only wrong he did was to exceed his scope of authority. The Second Circuit Court Judge rejected this line of reasoning by saying the Act only required an intent to access and not an intent to cause damage. The 1996 Act has made it explicit that such an argument was not possible under s1030 (5) (c).

* The Federal Sentencing Guidelines will supplement s1030 (c). It is aimed at assisting in determining the possible sentence a perpetrator should serve.

* On February 8th 1997, president Bill Clinton authorised the implementation of the Communications of Decency Act 1996 (CDA) that constitutes Title V of the Telecomunications Act 1996. The plaintiff was the American Civil Liberties Union which is composed of various organizations and individuals associated with computers who may publish or post materials on the Net. The defendants were Janet Reno who is the Attorney General of the United States and the United States Department of Justice itself. The plaintiffs argued that the censorship law under the

Act was unconstitutional. Dr. Donna Hoffman, an expert witness on marketing in cyberspace told the court that the censorship law destroyed the democratic nature of cyberspace causing many websites to be shut down because they fall within the definition of "indecency" which was given a vague meaning under the Act. Civil liberties or better said, cyberliberties were said to have been infringed. As a result, the Court severed the indecency restriction from the statute for such a restriction was said to infringe the rights of freedom of speech on the Net. But the Act criminalise the transmission of obscene materials to minors. However, the court suggested that a reasonable means of preventing children from accessing undesired or unwanted elements on the Internet will be for parents to use software programs that are designed for that purpose.

* [40]The Net has become dangerous to minors. This fear was expressed by the DOJ when it said,

"Never before in the history of telecommunications media in the United States has so much indecent (and obscene) material been so easily accessible by so many minors in so many American homes with so few restrictions." [41]Protection of Children From Sexual Predators Act 1998 aims to protect children from sexual predators in the following ways:

* by setting penalties for using the mail or any facility or means of interstate or foreign commerce to knowingly initiate the transmission of the name, address, telephone number, social security number, or electronic mail address of a person under age 16 with intent to entice, encourage, offer, or solicit any person to engage in illegal sexual activity;

* Provides for the prosecution of individuals for the production of child pornography if the visual depiction was produced with materials that have been mailed, shipped, or transported in interstate or foreign commerce, including by computer.

Besides legislative measures, other measures have been undertaken by the government.

The speech delivered by Robert S. Litt, Deputy Assistant Attorney General, Criminal Division of DOJ before the Subcommittee on Social Security Senate Ways and Means Committee on 6 May 1997 highlights some of these steps.

'.....we have long taken steps to ensure that the Justice Department can respond effectively to Net crime. For example, as far back as 1991 both the Federal Bureau of Investigation and the Justice Department created dedicated computer crime units. Since that time, the FBI has establishedtwo additional high-tech squads, and the Department has created within the Criminal Division, a new Computer Crime and Intellectual Property Section. Additionally, in early 1995, the Department of Justice initiated the Computer/Telecommunications Coordinator program, under which each of the 93 United States Attorney´s Office has designated at least one Assistant United States Attorney to serve as an in-house high tech expert. We provide special training to these prosecutors to help keep them a breast of the rapidly changing technological and legal issues. In addressing privacy concerns, the Department has participated in a number of working groups and forums that have included representatives from both the public and the private sector, including the Privacy Working Group of the Information Infrastructure Task Force. '

[42]More recent steps taken by DOJ to fight computer crime are centralised in its Computer Crime and Intellectual Property Section (CCIPS). It is responsible for lobbying for stronger penalties, for widening the coverage of federal computer crime statute and responsible for prosecuting computer crimes.

The National Infrastructure Protection Center (NIPC) is a joint effort of the DOJ, the Federal Bureau of Investigation (FBI) the DOD, the members of the business sector to assess and investigate threats to the information infrastructure.

[43]It was interesting to note that Title VIII of Protection of Children From Sexual Predators Act 1998 urges State Governors, legislators, and prison administrators to prohibit unsupervised access to the Internet by State prisoners. With these steps, it can be seen that the country is trying its best to keep these criminals at bay. Most of the other countries are also in the same position.

The United Kingdom and Cyberspace

Inadequacies that were highlighted in cases like [44]*R v Whitely* and [45]*R Gold & Schifreen* were rectified by the implementation of the Computer Misuse Act which came into effect in August 1990. The Act broadly makes three kinds of activities unlawful.

Browsing without lawful authority is known as basic hacking. It is an offence under s. 1.which states as follows:

1. (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 unauthorised; and

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

This is a summary offence whereby the sentences imposed are not very severe.[46]

Any form of hacking will fall under s.1 but if the offender has an intention to commit a further offence, he will be caught under s2 which states as follows:

2(1) A person is guilty of an offence under this section if he commits an offence under section 1 above ("the unauthorised access offence") with intent--

(a) to commit an offence to which this section applies; or

(b) to facilitate the commission of such an offence (whether by himself or by any other person); and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

Offences under s2 which carry a much higher sentence compared to s1. [47] S2 is worded in such a way that liability may be attached on the hacker without much difficulty. If for example, the hacker has obtained unlawful access, and has the intention to commit a further offence in the future, it still makes the hacker liable even if he did not commit the further offence at the time he was apprehended.[48]

If the hacker has obtained unlawful access, and has modified the data or has carried any unlawful alterations, he will be caught under s3 of the Act.

Section 3 is worded as follows:

3.--(1) A person is guilty of an offence if--

(a) he does any act which causes an unauthorised 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.

This section will apply if the modifications are unauthorised. This could apply under two circumstances. First, if person who makes the modification is not entitled to make the modification. Second, if the person making the modification does not have the consent from any person who is entitled to give the authority.

[49]The first case that was tried under s3 Computer Misuse Act 1990 was that of a virus writer. He had spread the viruses through the bulletin boards and had hidden the virus in computer games. Judge Jeremy Griggs said the following:

"Those who seek to wreak mindless havoc on one of the vital tools of our age cannot expect lenient treatment."

The Act has also dealt with jurisdictional issues. S 4 & s5 deal with problems that may arise due to the fact that the offence took place outside the United Kingdom . In essence both these sections say that the United Kingdom has only jurisdiction to try the offender if the offence is **significantly linked** to the United Kingdom. S5 states that it is possible under two circumstances listed under (2) (a) and (b) which states as follows:

5.(1) The following provisions of this section apply for the interpretation of section 4.

(2) In relation to an offence under section 1, either of the following is a significant link with domestic jurisdiction--

(a) that the accused was in the home country concerned at the time when he did the act which caused the computer to perform the function, or

(b) that any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in the home country concerned at that time.

One frightening feature of the computer crime, is the possibility that crimes may be committed across the border. A computer villain or vandal working at a computer in the United Kingdom may use his machine to commit crimes against computers located abroad in the belief that the United Kingdom does not have the jurisdiction to prosecute him. S5 clearly contradicts this belief. This means under s5 the vandal is within the jurisdiction of the United Kingdom and the English courts do have the powers to try the offender.

Effectiveness

After the arrest of Woods,[50] Detective Sergeant Barry Donovan who was formerly attached to the Scotland Yard´s computer crimes squad said that the arrest has drastically reduced the commission of hacking although hacking is an international problem.

The other legislation that has played a role in curbing these crimes is the Data Protection Act 1984.The Act regulated the use and storage of personal data. If a hacker has entered into a system where personal data is stored and he then makes a copy which is downloaded to the hacker´s computer, then the hacker is guilty under the Act. The Act makes it an offence to hold personal information without being registered under the Act. It also makes it an offence if the hacker is registered under the Act, but knowingly or recklessly obtains this data beyond the scope of his registration. An interesting case that may have fallen within the ambit of this Act is the [51]*DPP v Bignell*, where two police officers had asked two police computer operators to extract data from the Police National Computer (PNC) for personal purposes. They were initially tried under s1 Computer Misuse Act 1990, However, their conviction was quashed because being police officers they did have authority to obtain the data. Their access was not unauthorised as defined under s 17(5) of the Act. The reason for obtaining the data was not relevant. The course of actions that could have been

taken against them could have been to subject them to disciplinary action or/and to charge them under the Data Protection Act 1984. The latter view was rejected in a [52]subsequent case where the facts were similar. Here a police officer was convicted for improper use of personal data contrary to s5(2)(b),(3)and (5) Data Protection Act 1984. The House of Lords agreed with the Court of Appeal and held that the term 'use' should be given its ordinary meaning. It was held by the majority that retrieving information from the computer did not amount to the use of the information. This Act is to be amended by the Data Protection Act 1998 which became law on the 24th October 1998 and has been implemented since the 1st March 2000. This Act introduces a registered group f bodies called "Data Controllers" under the old Act s33 which exempted unincorporated clubs and societies. The extent of such an exemption under the new Act will be seen when the Act is tested before courts.

In addition to legislative measures, this study highlights a recent approach that the government has taken to keep up with the changes of computer technology. In 1998, the government stated its aim to make [53]" The United Kingdom the world´s best place to trade electronically by the year 2002". [54]To achieve this goal, (even if it may seen unrealistic due to the time factor) the Performance and Innovation Unit (PIU) carried out a study. The purpose of this study was to define the detailed and cross departmental strategy needed to ensure that this objective is reached.

The report highlighted three main areas which are as follows:

* to overcome business inertia;

* to ensure the Government´s own actions drive the take-up of e-commerce;

* To ensure better co-ordination between government and industry to gain maximum benefit from existing and proposed programmes.

It was recognised that there is not clear equivalence between written and digital documents under the English law. Thus laws that govern written documents cannot be applied to documents created due to e-commerce. Part II of the draft of Electronic Communications Bill which was presented to the House of Commons in 18 November 1999 was aimed to address this defect.

The other point that PIU highlighted was the protection of information by the Crown Copyright. Under the present system, the information is not so freely available to the private sectors unlike in the United States. It suggested that the approach used by the United States be adopted by the local governments. The system that is used in the United States is the Class Licensing System. This system covers anyone who republishes Crown copyright information, provided they meet the conditions of publications. If they fail to do so authorisation may be withdrawn.

Singapore and Cyberspace

The cyberlaws in the Asian region, are not extensive as in the United States or as in Europe. But there have been several laws in this area. The most prominent Act is Computer Misuse Act. [55] Despite the ineffectiveness of the Computer Misuse Act 1990, Singapore and Malaysia used that legislation to draft their respective Computer Crimes Acts. The Computer Misuse Act 1993 of Singapore was amended in 1998. It has only 16 sections. This Act has criminalised malicious attacks such denial of service attacks, the introduction of a definition of 'damage' as "any impairment to a computer or the integrity or availability of data, a program or system or information." Punishments such as a maximum of 20 years and fines up to 100,000 Singapore dollars imply that the overall objective of the Act is to prevent computer criminals walk free.

Electronic Transactions Act 1998

In 1998, the Electronic Transactions Act was passed. This Act is based on several US legislation and Article 1s5 of the German Federal Law of Commerce to Regulate conditions for Information and Communication Services[56]http://www.bakerinfo.com/publications/documents/606_al.ht[m]. It supports the electronic commerce in the following ways:

* Electronic transactions and documents are given the same legal effect as their paper counterparts.

* The determination of time, date and place when as electronic document or information is sent or received is clarified under the Act.

* Digital certificates will be issued by authorised agency, which will be recognised in other countries. The digital signature system will use an asymmetric cryptosystem.

* There will be a regulatory body, known as the Controller of Certification Authorities, whose duties will include the licensing, certification and the overseeing of the activities of certification agencies. There are the powers vested on the Controller. If users of computer or any other person who is in charge of computer fails to assist the Controller or if he obstructs investigations, he could be jailed for one year and fined up to 20,000 Singapore dollars.

This a relatively new Act. Whether it has flaws in its applications or otherwise can only be determined in the future.

[57]http://www.singapore.cnet.com/Briefs[/]When CNET Singapore interviewed Angelia Kho, a research analyst for the Gartner Group about the awareness in Singapore about computer security, This was her reply:

'Singapore´s efforts have been commendable so far.....it has set up the few vital foundations to ensure a safe and secure environment for electronic transaction. Through the National Computer Board (NCB), it has formed Netrust, a certification authority to address the management of issuing digital certificates for any e-commerce transactions. ....'

Malaysia and Cyberlaws

This article briefly outlines some of the cyberlaws passed by the Malaysian Government. There will be more laws of this nature passed in the future that will regulate the contents on the Net for instance.

The cyberlaws passed in 1997 are as follows:

* Computer Crimes Act which is yet to be implemented;

* Digital Signature Act which became effective from the 1st October 1998;

* Telemedicine Act which is also not in force yet;

* The Copyright Act was amended and it is now the Copyright (Amendment) Act which came into force on 1st April 1999.

* Malaysian Communications and Multimedia Commission Act which was implemented in 1998.

* These laws are believed to make the MSC (Multimedia Super Corridor) and the government´s vision of creating an electronic government a success. The Computer Crimes Act is yet to be implemented. The Act has only 12 sections and is rather comprehensive compared to the Computer

Misuse Act of the United Kingdom. Since it is not in force yet, its legal implications cannot be inferred yet. Wordings of s 3(1) Computer Crimes are very similar to s1(1) Computer Misuse Act 1990 of United Kingdom, but the difference lies in the sentence. The wordings of s(1) Computer Misuse Act 1990 of the United Kingdom are as follows:

1. (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 ordata held in any computer;

(b) the access he intends to secure is unauthorised; and

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

[58]The penalty for a s.1 offence of the United Kingdom is a maximum of six months jail or 5,000 pounds sterling or both. However under the Malaysian Act for the same offence the offender will be tried under 3(1) Computer Crimes Act 1997 which states as follows:

1) A person shall be 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 unauthorised; 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.

The [59] same offender in Malaysia is in much greater trouble for he may have to pay a fine up to RM 50,000 or be imprisoned up to 5 years or both! It is questionable if such severe punishments would serve any purpose, especially since hackers are commonly young persons.

The Digital Signature Act came into force on 1st October 1998. [60]It is said to be drafted after the Utah Digital Signature Act 1995 which is the first digital law in the world. Interestingly, this was also one of the Acts consulted when the Electronic Transactions Act 1998 of Singapore was drafted. It addresses digital signatures for business transactions that carried on over the Net. It also discusses the CA (certification authority). The functions of these bodies will be to certify and authenticate e-commerce by allowing the users to have a digital signature that is with the ambit of the Act. The Act also creates the office of "Controller of Certification Authorities" who has the powers to oversee and monitor the activities of CAs which will issue these certificates to subscribers. It is essential for a digital signature to be certified by the certification authority that is licensed. If this requirement is not complied with, the penalty is very heavy.[61] The offender may have to pay a fine up to RM 500,000 or face an imprisonment up to 10 years or both.

Telemedicine Act 1997 is a very "brief" Act. It has only six sections and is not in force yet. The Act may be simple but its existence shows the coming together of Information Technology (IT) and the

medical field to enhance the living standards of society. S 2 defines "telemedicine" as 'the practice of medicine using audio, visual and data communications.' With time, the Act will be `improvised' to cater for the discrepancies that will inevitably arise. For example the Act does not discuss jurisdictional issues.

The Copyright (Amendment) Act 1997 is another cyberlaw which came into force on 1st April 1999. It is a very recent Act which amended the 1987 Act. The new Act has amended nine sections of the old Act, deleted s21 and included a new section, 59B which discusses the power of the Minister in charge of copyright matters. This original Act was amended several times before.

This Act is aimed at overcoming the challenges that the MSC will bring. Listed below are some of the changes the Act has brought:

* The terms "fixation" and "literary work" are amended under s3(e) and (f) and the term "communication to the public has been introduced under s3(d). The term "broadcast" is redefined under 3(b) to include transmission by wire, visual images or sounds and the transmission of encrypted signals.

* S7 is amended by inserting after subsection (2) another subsection (2A) which reads as follows: "Copyright protection shall not extend to any idea, procedure, method of operation or mathematical concepts as such."

* [62]S41 is amended to include new offences under s41 (i) and (j).

If an Act has been drafted in such a manner that no criminal can find loopholes or weaknesses in the Act to take advantage and escape liability, it can be considered as an answer to some of the problems posed by IT. In fact all the cyberlaws of Malaysia are so new and they have not passed this acid test which can only be determined with time when cases come before the Malaysian courts.

Problems in Regulating the Cyberspace

Regulating cyberspace is one of the formidable tasks that countries around the world are undertaking. Governments are trying to align the Net to suit the norms and ideologies of their respective countries. These is not an easy challenge as pointed out by [63] Habib Al-Rida, Assistant Under-Secretary of the Ministry of Information, United Arab Emirates, who noted the following:

'The challenge facing us now is how to protect our society against the potentially harmful influences coming through the system, whether criminal or otherwise, while at the same time, making it possible for our companies and individuals to benefit form the valuable access to the worldwide pool of skills and information the Internetrepresents'

[64]Some countries may be over zealous in regulating the Net, the citizens in China for example, are restricted not only from accessing overseas pornographic websites but foreign news sources as well. (Time Warner´s AsiaNow site, which includes Asiaweek is among that is blocked).

Whatever the means may be, the most fundamental method would be to have laws that prevents "unwanted activities" on cyberspace. Laws deterring computer criminals have not in the past been very effective. In the [65]United States and the [66] United Kingdom, criminals have escaped despite the existence of such laws. This defect could be attributed to several factors one of it being the reluctance of judges and jurors when deciding the culpability of the offender when no physical or tangible damage has taken place. [67]In *US v Morris* the released a "worm" that spread to thousands of other computers and hindered the access by duplicating itself so mush that the computers crashed . The affected computer centres suffered many millions in lost time. A mere probationary sentence

may not have been meted out to another criminal if he had caused such a damage to a physical object. *R vCropp*[68] reflects the 'failure' of the Act was due to judicial interpretation. This would have been an outright unauthorised access. Yet the judge found defendant not guilty under s1 Computer Misuse Act 1990. S 1(1) (a) states as follows:

'causing a computer to perform any function with intent to secure access to any program or data held in any computer.' He construed this phrase to mean that more than one computer is needed for hacking to take place when he said:

'.....It seems to me to be straining language to say that only one computer is necessary..'

Jurors may share the same view, [69]*Bedworth* is an example of this phenomenon. They may have been reluctant to convict because the offender was a high school student. Computer hackers are often intelligent young persons who wish to challenge the limitations posed by the computer security systems. To criminalise their "innovative" abilities and to blacklist them as convicts may not be the ideal method to deal with the situation. Perhaps the governments concerned could take a more positive step by exploiting their intelligence and making them work for the government. Or make them unmake the wrongs that they have committed. This means the person who had spread the virus should be asked to remove it as well. This may be the antidote for situations like [70]*US v Morris.*

Key words like computers and data have not been defined under the Computer Misuse Act 1990. Such deliberate omissions many lead to incorrect or various interpretations which may complicate the problem at hand.

The major problem faced by all countries when it comes to IT is the necessity of computer literacy among the people who are responsible to bring about the conviction of an offender. Investigating computer crimes may be new to investigating officers. They need to be taught proper methods of collecting evidence from the computers. For if the computer is switched off, essential evidence may be lost or may become unreliable. Judges, police officers, the prosecution, witnesses and jurors need to be more e-inclined.

The effectiveness of the Act does not only depend on the wordings and the interpretation of the words but also on the understanding of an offence of this nature. This understanding can only be reached if persons involved in establishing the existence of a computer crime can prove to the jurors that a crime has taken place even though no physical damages can be detected. [71]There have been criticisms that the police lack the expertise to track hackers. [72]But subsequent prosecutions may show that the police is trying to do away with this image.

Under the Computer Misuse Act 1990, it is not an offence to write software virus programs. It is only an offence if the "virus" is passed into the computer systems. One may wonder if it would be more beneficial if the act of writing the "virus" itself should be considered as an offence. If this act is criminalised, then most spreading of viruses could be prevented at initial stages. Jurists may say that such a step could be drastic and the more appropriate approach would be try these offences as inchoate offences. In theory it may be possible, but no attempts have been done to prosecute the writing of virus programs as inchoate offences under the Computer Misuse Act.

To draft e-laws and to take other deterrent measures require the expertise and financial means. This factors do not pose problems to developed countries. However, for third world countries these may be serious setbacks in regulating cyberspace.

Global Initiations

The creation of the Internet has made computer crime a global problem. Domestic measures only will not address this global revolution. The recognition of this element has caused countries to work

together to overcome this 'adversity' of the Net. International problems require international solutions. [73]The North American Free Trade Agreement (NAFTA) is the first international agreement that was drafted to eliminate all bilateral tariffs and most non-tariff trade barriers between the United States and Mexico. It resolves international commercial disputes between private parties involving free trade. It has established an important Commission called the Free Trade Commission with oversight powers. The Commission has the powers to create bilateral or trilateral panels of private sector experts to resolve disputes. If this leads to a dead end, the parties can appeal to the government involved. The awards that are issued will be enforceable. If a nation has committed any kind of violation, it may be deprived of the benefits that it has obtained under the agreement. Expanding such agreements to other countries will have many benefits such as an increase in trading and creation of job opportunities.

International resolutions are also present in the European region and this was seen in one of the responses of the European Commission Communication Paper which stated as follows:

[74]www.leeds.ac.uk/pgs/yaman/watchmen.ht[m]*"the answer to the challenge will be a combination of self-control of the service providers, new technical solutions such as rating systems and filtering software, awareness actions for parents and teachers, information on risks and possibilities to limit these risks and of international co-operation."*

[75]One of the recent international co-operation was the International Guidelines Issued for Consumer Protection in E-Commerce.(OECD) These guidelines were adopted by the OECD on 9th December. It was for consumer protection in e-commerce. Primarily, the guidelines stipulate the following:

* a means for governments and businesses on how to establish electronic commerce

* providing on-line shoppers the same protection as off-line shoppers.

The United States Federal Trade Commissioner Mozelle W. Thompson who led the United Sates delegation in the OECD, made the following observation:

The guidelines "contain the building blocks to develop that confidence in a global elctronic market"

However, these guidelines do not have binding effects on its members countries. But the European Commission in a separate statement shares the spirit of the OECD. Health and Consumer Protection Commissioner David Byrne expressly made this point when he said that these guidelines closely reflect European Union´s consumer protection regulations and principles.

These guidelines could be the basis 'International Cyberlaws'. The terminology may be a misnomer but the existence of such global jurisdiction would be necessary as these laws consider the computer crime as a global problem or disaster rather than a domestic issue. Such a broad perception will certainly be beneficial to address global issues.

Conclusion

The Net has created a new wave of information distribution that transcends geographical and political borders. It is difficult to control this new space which accommodates the reservoir of information, be it by legislative or technological means. However these difficulties should not be misconstrued or considered as setbacks. However, they should be taken up as challenges posed to the governments of the day and to international organisations to motivate them to come up with up-to-date means and methods that would keep cybercriminals away from cyberspace.

[1] Martin Wasik, Crime and the Computer (1990) p 33, Clarendon Press.

[2] Yochait Benkler, Rules of the Road for the Information Superhighway: Electronic Communication and the Law, at pp. 1-2.

[3] Newsweek. 11 October 1999.

[4] <http://www.cert.org/research/JHThesis/start.html>

[5] New Straits Times 10 February, 2000.

[6] Tapper {1987] Crim L Rev 4. Describes the phrase11 as 'ungrammatical and inelegant'

[7] National Institute of Justices, U.S. Dept´s of Justice COMPUTER Crime: Criminal Justice Resource Manual 2 (1989).

[8] R v Gold (1988) AC 1063. The defendant was acquitted since there were no laws to prevent unlawful access.

[9] R v Whitley (1991) 93 Cr App Rep 25, the defendant was charged under the Criminal Damage Act for when a computer´s storage medium was impaired by altering the storing magnetic particles.

[10] Supra 8, the password was 22222222 and the user id was 1234.

[11] Julie Tamaki, Famed Hacker is Indicted by U.S. Grand Jury, L.A. Times, Sept. 27, 1996.

[12] In one case, a disgruntled employee, Donald Burleson, upset over his termination, copied and then deleted 168,000 sales commission records in the hopes of being reinstated, When this did not happen, he crashed the company´s computer system. He was convicted, fined and sentenced to 7 years probation. (Burleson v State, 802 S.W. 2d 429.)

[13] R v Thompson [1984] 1 WLR 926.

[14] A joint study of the Business Software Alliance (BSC) and the Software Publishers Assiciation (SPA) estimated that illicit software pirating alone cost American businesses 11.4 billion US dollars in lost revenue in 1997. *Reuters, Technology Software Priacy Estimated at 11.4 billion US dollars* L.A. Times, June 17, 1998.

[15] <[>

16] The Times of London, 22 November , 1997.

[17] US V Morris 928 F 504 (2nd Cir 1991) .

[18] United States General Accounting Office, Information Security: Computer Attacks at Dept. of Defense Pose Increasing Risks. (hereafter Information Security)

[19] Information Security, See also Scoot Mooneyhan, Soldier Acquitted of Spying, Gets 3 Years on Lesser Charges, NEWS TRIB.

[20] Peter Warren Computing (1996).

[21]Unreported, Plymouth Crown Court, May 1995. See guardian, 16 November 1995.

[22] This decision was overruled by the Court of Appeal in Attorney General´s Reference (No 1 of 1991) (CA) (1992) 3 WLR 432.

[23] "Bedworth case puts law on trial" *Computing* 25 March 1993 p7.

[24] Andrew Charlesworth, *Between flesh and sand: Rethinking the Computer Misuse Act 1990,* International Yearbook of Law, Computers and Technology, 1995, Vol9, p31.

[25] [1989] Crim L Rev 309.

[26] Klaus Brunnstein and Simone Fisher-Heuber, How far can the criminal law help to control IT misuse? International Yearbook of Law, Computers and Technology, 1995, Vol 9.

[27]<[.cnet.com/Briefs/Guidebook/Crime0814/ss01.html>

28] News Straits Times 30 January 2000.

[29] Virus is a hidden computer program that can replicate itself and attach itself to other programs.

[30] Trojan horses are computer programs that appear to be innocent but cause damage.

[31] Logic bombs are activated if a particular event takes place, until then they are dormant.

[32] US v Peterson, 98 F 3d 502, 504 (9th Cir 1996).

[33] Dodd S. Griffith. The Computer Fraud and Abuse Act of 1986: A measured Response to a Growing Problem, 43 Vand. L Rev 453, 455 (1990).

[34] 18 U.S.C. 1030 et seq. (1988).

[35] Pub. L. No. 100-690, Title VII, SS 7065, 102 Stat. 4404 (1988) [hereafter 1988 amendments].

[36] Henry H. Perritt, Jr., Law and the information superhighway 571 (1996).

[37] A negligent violation is a misdemeanor under 18 U. S. C.A s1030 (c) (2) (A). (Supp. 1998)

[38] A reckless violation is a felony see 18 U.S.C.A s1030 (c) (3) (A) (Supp. 1998).

[39] Supra 17.

[40] U.S. Department of Justice, Post Hearing Memorandum of Points and Authorities, at 1, ACLU v Reno 929 F. Supp. 824 (1996).

[41] <http://www.prevent-abuse-now.com/law2ac.htm>

[42] <http://www.usdoj.gov/criminal/cybercrime/195 ag.htm>

[43] <http://www.prevent-abuse-now.com/law2.ac.htm>

[44] Supra 9.

[45] Supra 8.

[46] 1 (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.

[47] S2(5) A person guilty of an offence 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.

[48] s2(3) Computer Misuse Act 1990.

[49] Supra 21.

[50] Strickland and Woods were sentenced to six-months in prison at Southwark Crown Court on 21st May 1993.

[51] In various articles 'Bingell' is spelled as 'Bingall' This paper follows the report of The Times, 6 June 1997.

[52] (R v Brown, The Law Reports[1996] 1 AC.)

[53] Government White Paper "Our Competitive Future - Building the Knowledge Driven Economy" CM 4176 December 1998.

[54] December 1999 - January 2000 - World InternetLaw Report.

[55] Supra 23.

[56]< [>

57] <[Guidebook/Crime0814/ss01.html>

58] S1(3) CMA 1990.

[59] S3(3) CCA 1997.

[60]< http://www.malaysia.net/dap/sg329.htm>

[61] s4(2) Digital Signature Act 1998.

[62] 41(i) removes or alters any electronic rights management information without authority; or 41(j) distributes, imports for distribution or communicates to the public, without authority, works or copies in respect of which electronic rights management information has been removed or altered without authority.

[63] Ahmad Mardini, Gulf-Culture:Officials Worry About Smut on Internet, InternetPress Service, January 19, 1996.

[64] Asiaweek 11 February 2000.

[65] Supra 17.

[66] Supra 23.

[67] Supra 17.

[68] Supra 22

[69] Supra 23.

[70] Supra 17.

[71] See eg, Andrew Charlesworth, Between Flesh and Sand : Rethinking the Computer Misuse Act 1990 International Yearbook of Law Computers and Technology,1995, Vol 9, 31 at 36.

[72] Supra 21.

[73] <http://www.law.ttu.edu/cyberjou/jour21.htm>

[74] <http://[>

75] December 1999-January 2000 World InternetLaw Report.