Technical Report

Research Project

Identification Of Appropriate Technologies and Procedures For Handling Digital Evidence

Chief Investigator
Sh Ashok Dohare
Co-investigator
Shri Rakesh Aggarwal
SVP National Police Academy Hyderabad

Research Project Funded
By
Department of Information Technolgy
Ministry of Communication and Information Technology
Government of India

Technical Report

Identification of Appropriate Technologies and Procedure for Handling and Analysising Digital Evidence

Ashok Dohare
Rakesh Aggarwal

Table of Contents

Annexures

Acknowledgements

This whole endeavor started as a result of a brief interaction, Ashok Dohare had with Dr A B Saha, and Shri A S A Krishnan both from Ministry of Information Technology way back in the year 2002, during a National Seminar held in Hyderabad, in which he had presented a paper titled: Information Technology Act 2000 – Issues and Challenges. I am grateful to Department of Information Technology, Ministry of Communication and Information Technology, to have funded the project *"Identification of appropriate technologies and procedures for handling and analyzing Digital Evidence".* The financial grant was of Rs Fifty Lakhs Simultaneously, DIT, sponsored another project, at ER&DCI Trivandrum (Now C-DAC) for developing a software to seize, acquire and analyze Digital Evidence based on the specifications finalized and agreed upon as a deliverable of the first project.

We are grateful to Prof N Balakrishnan, Supercomputer Education and Research Centre, IISc. Bangalore, Dr G Athithan, CAIR, DRDO Bangalore, Prof N Krishnan, AU-KBC MIT Chennai, Sh R Krishnamurhty, IISc. Bangalore, Shri P Krishnasastry GEQD Hyderabad, and all the other members of the Project Review and Steering Committee for their guidance and encouragement.

We duly acknowledge, with thanks, the encouragement, support, and for all the financial help received from Shri Rajeeva Ratna Shah, former Secretary DIT, Sh M K Shukla former Director SVPNPA, Sh Ganeshwar Jha Director SVPNPA, Shri SS Jaiswal, Secretary DIT, Shri Laksmi Narayanan Addl Secretary DIT, Dr A K Chakarvarti Advisor DIT, and Shri S Basu Sr Director DIT.

Thanks are due to Sh N Krishnan and his team from C-DAC, specially Shri B Ramani, Shri K L Thomas, Shri V K Bhadran and Shri C Balan for accomplishing the Herculean task of developing the Tool - CyberCheck, as per the specifications.

Sincere thanks to Sh Vepa P Sarathi Senior Advocate, Smt Radha, Research Associate, Smt Laxmi, Research Assistant and Shri N V Abraham for their valuable contributions in the successful completion of the project.

A study of this nature cannot be completed without a number of people helping out, directly or indirectly. Sincere gratitude, especially to all officials of Ministry of Home Affairs, CBI, and other senior police officers who visited the Cyber Forensics Laboratory SVPNPA, established from the funds of this project for their appreciation and encouragement. The study is largely based on the material available on the Internet, which were consulted during the course of the research. The authors of those articles, who made their views and finding freely available for the growth and development of the emerging subject of Digital Forensics, are the most to be thanked.

All this was made possible by the efforts of Shri ASA Krishnan Director DIT, who successfully coordinated the efforts of the two groups, culminating in the present work. His pain staking efforts are duly acknowledged.

Rakesh Aggarwal

Ashok Dohare

The Project Review and Steering Group

The project was Guided and continuously reviewed by the committee which constituted as follows

Dr G Athithan	CAIR DRDO Bangalore	Chairman
Shri R Krishnanmurthy	SERC IISc Bangalore	Member
Shri N Krishnan	C-DAC Trivandrum	Member
Shri S A Kumar	Cabinet Secretariat	Member
Smt Sundari Nanda	Cyber Crime Cell CBI	Member
Shri Krishnasastry	GEQD Hyderabad	Member
Shri ASA Krishnan	DIT, MCIT Delhi	Member Secretary

Research Team

Shri Ashok Dohare	Deputy Director SVP NPA	Chief Investigator
Shri Rakesh Aggarwal	Asstt Director SVP NPA	Co-Investigator

Scope and Objectives of the study:

Crime follows opportunities. More the opportunities, more and more people offend to commit crime. Thus one of the fundamental principles for prevention of crime has been opportunity reduction, which translates to having better and better security. However, this is only one of the aspects in the whole gambit of prevention of crime. The other two aspects viz., 1. Probability of apprehension of the criminal and thereafter a successful conviction are the other two major deterrents. This requires having adequate laws clearly defining criminal misconduct, criminal conduct and sound procedures for the criminal trials to be conducted successfully in the court of law. Convictions every depend on presentation of evidence in a manner that it is admissible in a court of law, is authentic and reliable. This involves developing procedures for identifying and handling digital evidence.

The study is conducted into the following objects:

a. To make a comparative study of
   1. The various IT Laws Enacted / Proposed in various Countries in the World
   2. The recommended Procedurals Laws with respect to Digital evidence in Various Countries of the World
   3. Identification & Study of various Technologies in use for handling & processing Digital Evidence

b. And thereafter make recommendations regarding

a. Amendments if any, in the IT Act 2000 and other penal laws, specially with respect to dealing with Computer Related Crimes

b. Required amendments to the procedural Laws, specially the CrPC

c. Identification of appropriate Procedures for handling / processing Digital Evidence

d. Identification / Development of appropriate Technology for handling / processing Digital Evidence.

The study is limited to off-line forensics of stand alone computers.

INTRODUCTION:

One of the most significant and influential inventions of the 20th century, which was full of innovation, and inventions, was the Computer and the Internet. The primary role of today's computer is certainly not what its early inventors envisioned. It has metamorphosed from a giant calculating machine to a stand alone personal tool after forming a sorted routine tasks like a word processing and book keeping, to today's network device permitting virtually instantaneous and global personal, corporate and governmental interaction. The story of Computers, computing, and networking has been one of evolution of purpose. The calculating machine has become the portal to a new world of human activity, a world different in so many essential ways, everyday world that we have named this new place as "Cyber Space". While providing tangible benefits in providing time and money, the computer has an impact on everyday life, as computerized routines replace mundane human tasks. More and more of our businesses, industries, economies, hospitals and governments are becoming dependent on computers. With the computer, the heretofore impossible has become now possible. The computer is allowed large volume of data to be reduced to high density, compact storage nearly imperceptible to the human senses. It has allowed an expiation increase in calculating speed, worldwide connectivity and communication. The Cyber Space, a virtual domain is a place populated by human minds since it is our intellects that reside and need one another there. Cyber Space is a domain that exists along with, but apart from the physical world making it a shared conceptual reality. It should come at no surprise, then, that many of the problems of the real world carry over into this new realm. Crime is one of them. It has opened the door to anti-social and criminal behavior in ways that would never have previously been possible. Some Cyber Space crimes such as unauthorized access to a computer, a new and specific to the online world, others such as fraud or theft of valuables are familiar from the real world. In either case, the disc embodied often-anonymous nature of activity in Cyber Space creates problem in enforcing law. Laws, criminal justice system and international cooperation have not kept space with technological changes to an extent that even now, nations are trying to develop laws and procedures to combat the menace of Cyber Crimes and resolve all of the legal enforcement and prevention problems.

The rapid transnational expansion of large-scale computer networks and the ability to access any system through regular telephone line has transformed the world into a global village bringing within its ambit our country also. India too, has enacted the Information Technology Act 2000 to harness the Information Technology revolution. The Act primarily aims at legalizing the two emerging technologies viz., electronic commerce and electronic governance both conducted through the electronic media.

Both e-governance and e-commerce revolve around Computers and Internet. Internet, was designed on the following four premises:

1. Each distinct network would have to stand on its own and no internal changes would be required to any such network to connect to the Internet.
2. Communication would be on a best effort basis. If a packet did not make it to the final destination, it would shortly be retransmitted from the source.
3. Black boxes would be used to connect the networks; these would be later called gateways and routers. There would be no information retained by the gateways about the individual floor packets passing through them

thereby keeping them simple and avoiding complicated adaptations and recovery from various failure modes.

4. There would be no global control at the operational level.

The above made the Internet vulnerable, the vulnerabilities being commonly referred to as PAPA i.e., Privacy, Accuracy, Property, and Accessibility. Before these vulnerabilities could be effectively addressed, use of Internet for e-commerce and e-governance compounded the problem further since these technologies required effectively addressing the following issues also.

1. Authenticity
2. Integrity
3. Confidentiality
4. Non-repudiation

It is because of these vulnerabilities that Cyber Space is the scene of virtually every level of wonderful activities. It would be wrong on our part to hypothesis that Internet has given us new kinds of crimes and new types of criminals. In fact Internet has given our societies lawless fringe a new environment and some new tools for people to commit crimes. What we seen in Cyber Space, often-in dramatic ways are simple new expressions of traditional criminal mindset and conduct. The Internet is just another playing field for the criminals. The need of the hour is to shrink the societies lawless fringe by having adequate laws to harness conduct which constitutes a crime in the Cyber Space.

The Act recognizes documents generated stored and communicated in the digital form. It amends the major penal laws of the country viz., Indian Penal Code, Indian Evidence Act, Bankers Book Evidence Act and the Reserve Bank of India Act 1934. It legalizes digital records as evidence. Evidence is the foundation for identifying apprehending and prosecuting criminals. Forensic sciences had developed well-understood techniques for dealing with real world evidence. The question being confronted is

1. What must investigators do to collect preserve and authenticate digital evidence?
2. How can legal admissibility of legal evidence be assured?
3. How can digital evidence be used to reconstruct crimes and generate investigative needs?

The present study is an attempt to answer the issues enumerated above.

Evolution of Law relating to Computer related Crimes

It is difficult to determine when the first crime involving a computer actually occurred. The computer has been around in some form since the abacus, which is known to have existed in 3500 B.C. in Japan, China and India. In 1801 profit motives encouraged Joseph Jacquard, a textile manufacturer in France, to design the forerunner of the computer card. This device allowed the repetition of a series of steps in the weaving of special fabrics. So concerned were Jacquard's employees with the threat to their traditional employment and livelihood that acts of sabotage were committed to discourage Mr. Jacquard from further use of the new technology. A computer crime had been committed.

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

It was not before the mid-1970s that the first empirical computer crime studies applying scientific criminological research methods were conducted. These studies brought to light a limited number of verified computer crime cases, but at the same time suggested a high estimated number of undetected or unreported cases of computer crimes.

The public and scientific view of computer crime radically changed in the 1980s, when the press published astonishing cases about hacking, viruses and worms. Furthermore, a broad wave of program piracy, cash dispenser manipulation and telecommunication abuses revealed to a broad public the vulnerability of an information society and such also the need for a new strategy of Data Processing security and crime control. Computer crime was no longer limited to economic crime, but included attacks against all kinds of interests, such as the manipulation of a hospital computer or computer-related infringements of privacy. Thus, it became clear that the notion of computer crime had to be established as a broad concept, which, later in the 1990s, could integrate the distribution of illegal contents on the Internet as well as include the use of computers and communication systems by groups of organised crime.

A definition for Computer Crimes

As a consequence, in 1983 a group of experts of the OECD defined the term "computer crime" (or "computer-related crime") as any illegal, unethical, or unauthorized behaviour involving automatic data processing and/or transmission of data. Later studies went even further in developing broader concepts on "data and/or information crime". The breadth of these definitions proved to be advantageous as it allowed the use of the same working hypothesis for all kinds of criminological, criminalistic, economic, preventive and legal studies.

The concept of computer-related criminal law has undergone similar changes as the concept of computer-related crime: Many of the above-mentioned new forms of crime led to new computer-specific legal questions and law reform, thus broadening the concept of computer-specific criminal law and legislation. Especially since the 1970s, there have been a growing number of law reform projects in many countries.

The reason for this adaptation of the law to new forms of crime was not only based on technical changes, but mainly on fundamental changes of paradigms: Until the middle of the 20th century, the criminal codes of all countries have predominantly protected tangible objects. However, towards the end of the 20th century, the emerging information society has led to an increased importance of incorporeal values and information. These new values could not be protected in analogy to corporeal objects, but required new legal provisions. Thus, the field of computer-related criminal law soon became a complex field of many different new legal questions.

The Importance of Adequate Legislation to Address Cyber Crimes

Grabosky and Smith (1998) identify the following categories of crime emerging in the digital age: illegal telecommunications interception; electronic vandalism or terrorism; theft of communications services; telecommunications and associated intellectual property piracy; electronic distribution of pornography; electronic fraud; electronic funds transfer crime; and money laundering. While many of these categories of crime can be prosecuted under a combination of existing criminal, commercial and intellectual property laws, it is clear that additional legislation is often required in order to deal with certain kinds of computer-related illegalities. These crimes are becoming increasingly referred to as "cybercrimes".

The facets of Cyber Crimes

While there is no universally accepted general definition of cybercrime, much less national legislation explicitly employing the term, it can be seen that cybercrime comprises two overlapping domains.

The first is illegal **activities directed at or perpetrated through the use of computers**. This can include theft of computers, willful damage to computers or computer systems, unlawful access to or interference with the operation of computers, transmitting offensive or illegal content using computers, and committing fraud or other offences through the use of computers (Sieber 1998; United States Department of Justice 2000; Grabosky, Smith & Dempsey 2001).

A related area is the **protection of information**. This has been a concern of legal systems from well before the introduction of modern technologies of mass communication, but is clearly brought into focus by the development of global computer-based information networks such as the World Wide Web and the Internet (Tan 2000). Principal legal measures related to the protection of information from unlawful use, distribution or exploitation include intellectual property laws, privacy laws, laws relating to secrecy and national security, and laws relating to unfair commercial advantage.

Need for harmonization between the different national criminal and procedural law:

The problem faced by the investigating agencies while investigating and tracking down the person who created the love bug virus is the fine illustration and is instructive for those who are concerned about Cyber Crimes because it clearly illustrates some of the problems this type of activity poses for Law Enforcement officials.

1. The lack of Cyber Crimes specific panel laws and/or inadequacy of penal laws.
2. The lack of international agreement on Cyber Crimes which exacerbates the problems posed by lack/inadequacy of local penal law and often conflicting requirements of local procedural laws.

3. The difficulty of ascertaining jurisdiction and asserting jurisdiction especially because of no consensus on extradition and natural assistance treaties.

Cyber Crimes are a challenge for every nation; a challenge countries have to address both individually and collectively. Individually each nation must examine its own penal and procedural law to determine whether they are adequate for dealing with Cyber Crimes. Because technology has made national boundaries permeable, Cyber Crime is not a phenomenal that can be dealt with only at the national level. The emergence of Cyber Crimes we witness the correlate development of remote offenders who can while physically located in one country easily wreak havoc in other nations. International cooperation is required to deal with the Cyber Crimes as a transnational phenomenon. Nations must cooperate to deal with problems of Cyber Crimes by ensuring that Cyber Criminals cannot exploit gaps and loopholes in criminal and procedural laws to evade arrest and prosecution.

Despite the multitude of new computer-specific legal questions, the emergence of computer-related criminal law (or criminal information law) can be systematized and traced back to six main waves of computer crime legislations, which today still characterize the six main fields of criminal information law and therefore can be the basis of a study on evolution of laws relating to computer-related crimes. The enactment of laws / legislation could place independent to above differentiations, an differential study keeping the above categorization can be tabulated as follows

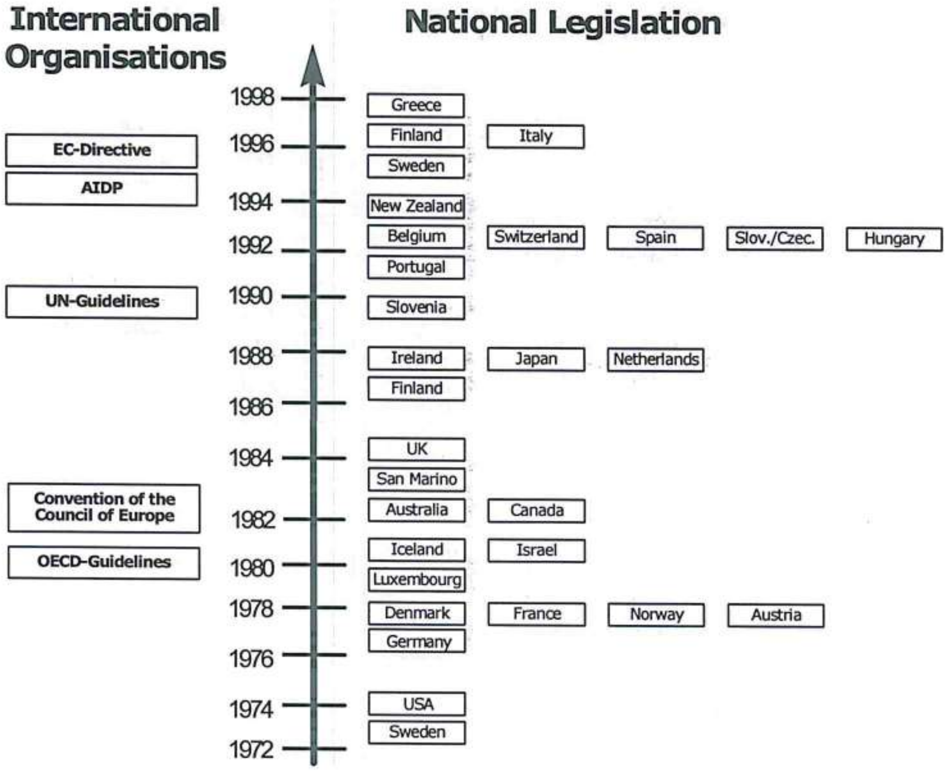
1. Protection of privacy: The laws primarily addressed to protection of journal administrative and civil data protection.
2. Economic criminal law primarily addressing to computer related economic crimes.

3. Protection of intellectual property primarily dealing with issues of intellectual property protection.
4. Illegal and harmful contents primarily regulating the illegal and harmful contents placed/communicated over the communication media.
5. A criminal procedural law
6. The security law dealing with security regulations especially with respective cryptography.

a. Protection of Privacy

Primarily General Administrative and Civil Data Protection Law

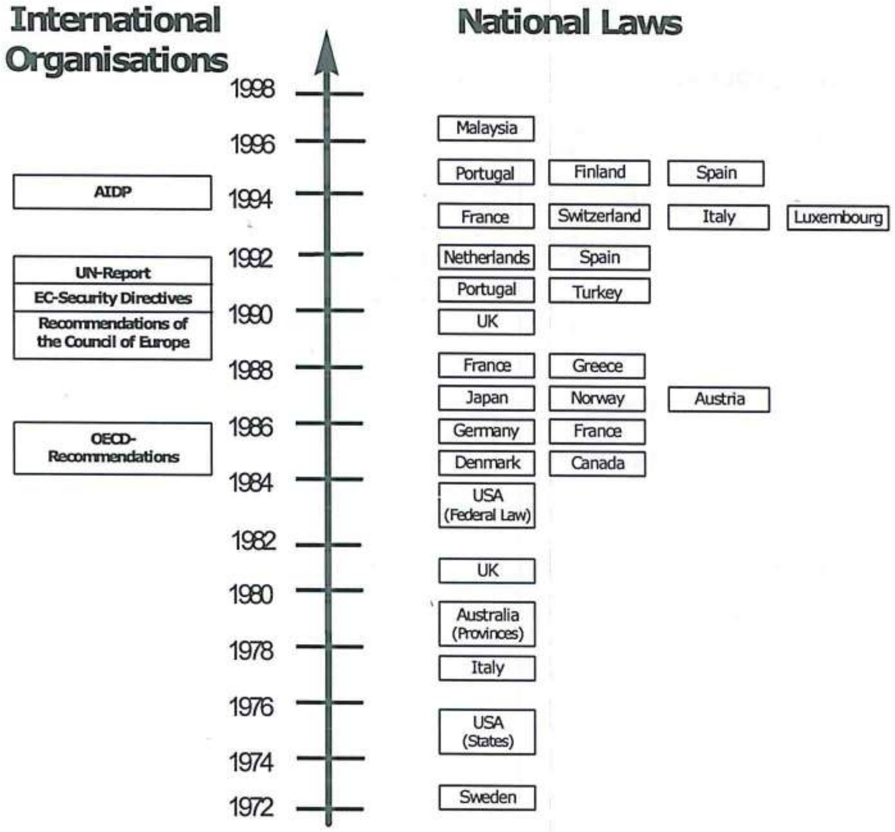
Swedan and US were among the first countries to bring out legislation on this issue. OECD issued the first ever guidelines for member countries in 1980. the latest guidelines have been issued by European Council for Cybercrimes.



b. Economic Criminal Law

Computer-Related Economic Crime

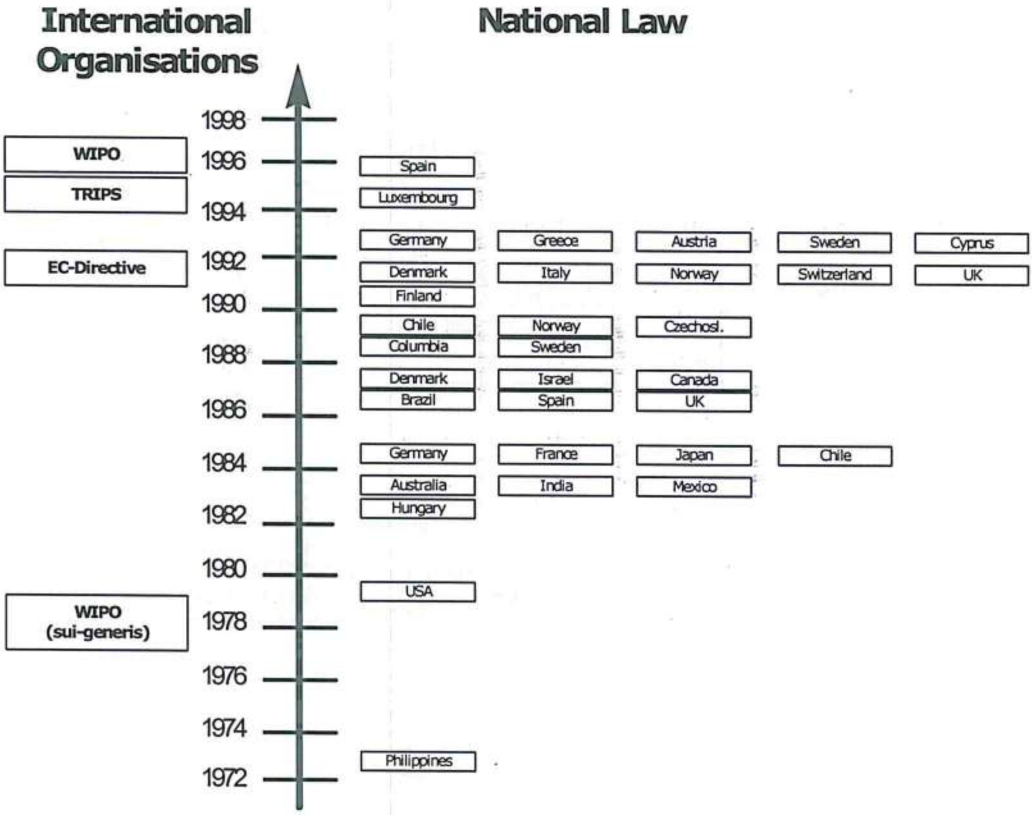
In view of the threats and the importance, US legislated a Federal legislation on this issue in the year 1984



c. Protection of Intellectual Property

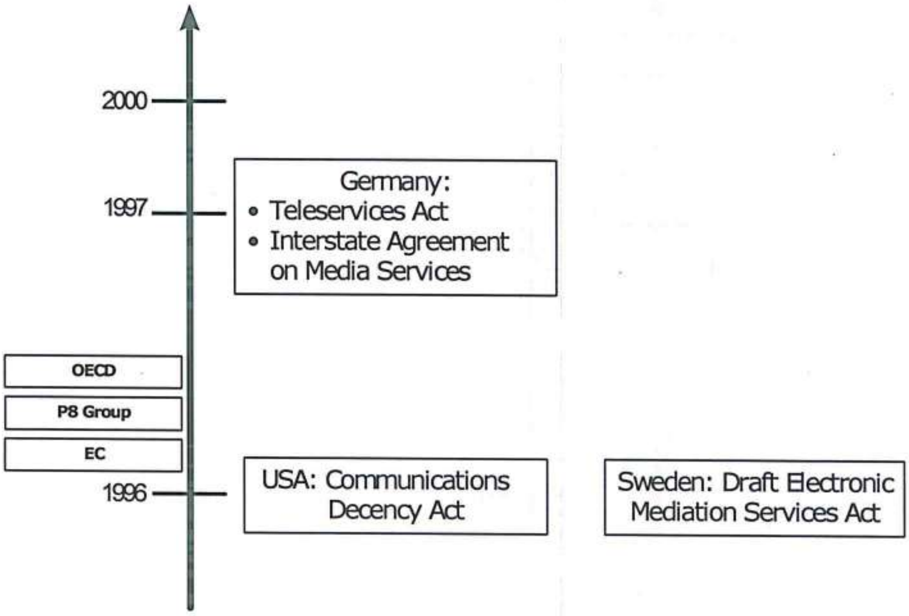
Intellectual Property Protection (Using the Example of Copyright Protection of Computer Programs)

The Latest Guidelines are those released by WIPO

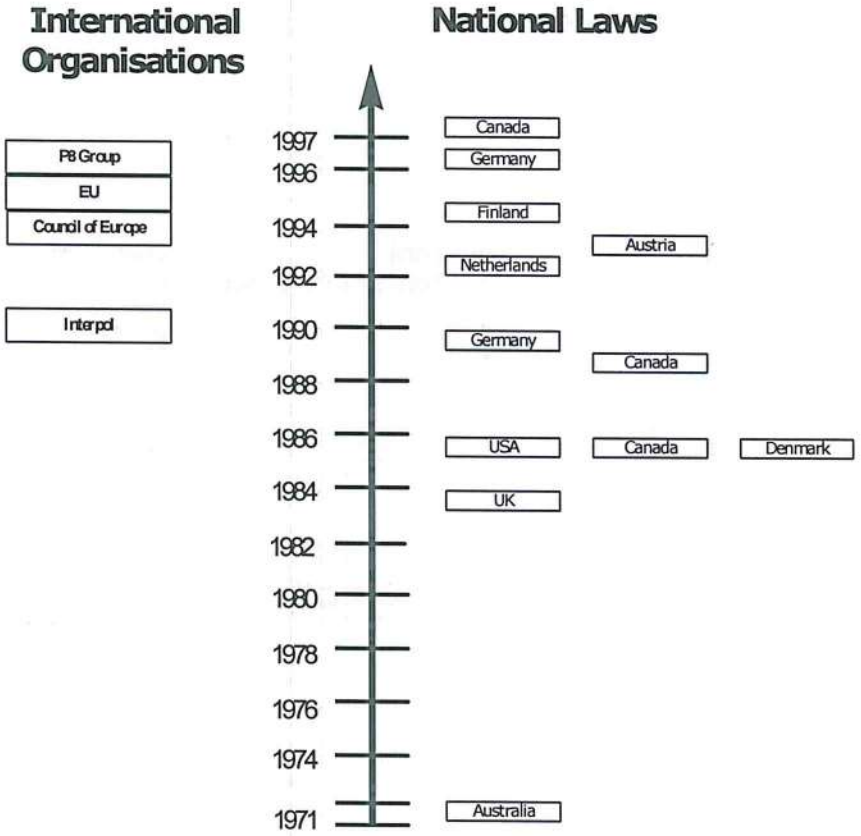


d. Illegal and Harmful Contents

Illegal and Harmful Contents (Using the Example of Responsibility of Access and Service Providers)

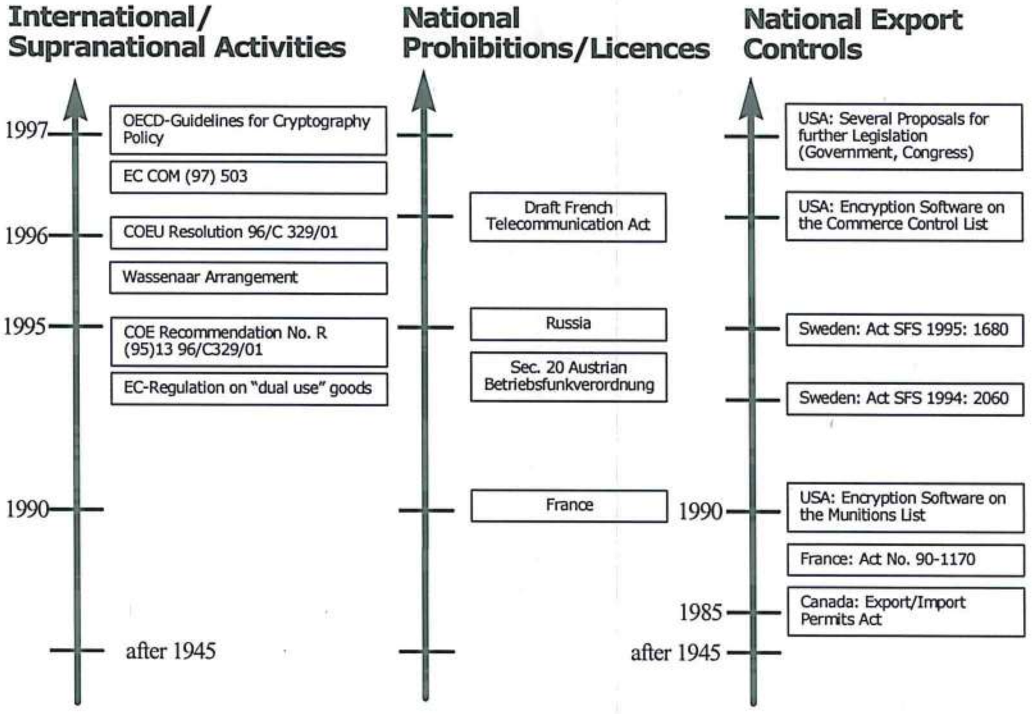

2000
1997
1996
Germany:
• Teleservices Act
• Interstate Agreement on Media Services
OECD
P8 Group
EC
USA: Communications Decency Act
Sweden: Draft Electronic Mediation Services Act

e. Criminal Procedural Law



f. Security Law

Security Regulations (Using the Examples of Prohibitions and Export Controls for Cryptography)


International/ Supranational Activities
National Prohibitions/Licences
National Export Controls
1997
1996
1995
1990
after 1945
OECD-Guidelines for Cryptography Policy
EC COM (97) 503
COEU Resolution 96/C 329/01
Wassenaar Arrangement
COE Recommendation No. R (95)13 96/C329/01
EC-Regulation on "dual use" goods
Draft French Telecommunication Act
Russia
Sec. 20 Austrian Betriebsfunkverordnung
France
USA: Several Proposals for further Legislation (Government, Congress)
USA: Encryption Software on the Commerce Control List
Sweden: Act SFS 1995: 1680
Sweden: Act SFS 1994: 2060
1990
USA: Encryption Software on the Munitions List
France: Act No. 90-1170
1985
Canada: Export/Import Permits Act
after 1945

International Trends and Conventions.

International organizations like O.E.C.D., Convention of Council of Europe, The United Nations, A.I.D.P., W.I.B.O., TRIPS, P8 group, have played a major role in harmonization of laws and procedures throughout the world.

A more systematic international understanding of the legal aspects of cybercrime is emerging through sources such as:

i. the Council of Europe's *Draft Convention on Cybercrime* (Council of Europe 2001);

ii. the United Nations symposium on "The Challenge of Borderless Cybercrime" held in conjunction with the Palermo signing conference of the *Convention Against Transnational Organised Crime*

iii. the United States President's Working Group on Unlawful Conduct on the Internet (United States Department of Justice 2000);

iv. cross-national comparative studies such as *Cyber Crime ... and Punishment? Archaic Laws Threaten Global Information* (McConnell International 2000).

The most significant international development is the Council of Europe's *Convention on Cybercrime* (final draft released on 25 May 2001). The text, which has taken almost four years and many redrafts to reach its present form, was approved by the Parliamentary Assembly (24 April 2001) with recommendations to include provisions on human rights and a protocol to ban "hate speech", and adopted by the European Committee on Crime Problems at its 50th plenary session (18–22 June 2001). The final draft was submitted to the Committee of Ministers for adoption during its 109th Session, on 8 November 2001.

The Convention was the first international treaty to address criminal law and procedural aspects of various types of criminal behavior directed against computer systems, networks, or data and other types of similar misuse. Signatories to the Convention include the 43 member states of the Council of Europe plus the United States, Canada and Japan.

The Europe's Convention on Cyber Crimes identifies the following as offences which should be incorporated into substantive criminal law in participating countries (Council of Europe 2001, Chapter II).

Offences against the confidentiality, integrity and availability of computer data and systems (Title 1)

i. Illegal access (Art. 2)
ii. Illegal interception (Art. 3)
iii. Data interference (Art. 4)
iv. System interference (Art. 5)
v. Misuse of devices (Art. 6)

Computer-related offences (Title 2)

i. Computer-related forgery (Art. 7)
ii. Computer-related fraud (Art. 8)

Content-related offences (Title 3)

i. Offences related to child pornography (Art. 9)

Offences related to infringements of copyright and related rights (Title 4)

i. Offences related to infringements of copyright and related rights (Art. 10)

Ancillary liability and sanctions (Title 5)

i. Attempt and aiding or abetting (Art. 11)
ii. Corporate liability (Art. 12)

Chapter II of the Convention goes on to canvass procedural matters such as collection and preservation of evidence, production orders, search and seizure, data interception and jurisdictional issues. Chapter III deals with mechanisms for international cooperation (Council of Europe 2001).

The legal analysis that follows adopts the Council of Europe's classification of computer offences. The study excludes the offence provisions under national intellectual property laws.

Comparative Study of Penal Laws

Adequacy of Legislations

Countries can be initially categorised according to whether they have:

i. basic criminal and commercial laws;

ii. a developed system of intellectual property laws; and

iii. legislation directed specifically at computers and electronic commerce.

Each of the countries considered below may be observed to fall within one or more of these categories, with most satisfying the second category and having made some progress towards the third. Whether the existing legal system in any country can adequately address cybercrime depends on the precise scope and interaction of its criminal, commercial, intellectual property *and* computer-related laws. As a general rule, however, the development of each of the later categories has been necessitated in part by the perceived inadequacy of legal remedies provided by other categories. The reliance on specific intellectual property laws to protect valuable information, for example, is partly attributable (in jurisdictions based on the English legal system) to the common law doctrine that information is not property capable of being stolen. Thus, information piracy is not amenable to prosecution under the criminal law relating to theft or dishonest acquisition (Grabosky & Smith 1998, Chapter 5). In many countries there are also difficulties in prosecuting under criminal law acts which may be performed outside the jurisdiction but which result in harm within the jurisdiction, such as the posting of offensive or obscene content on the Internet.

Clearly, there are also significant differences in the legal, social and political contexts within which these laws have been formulated and are enforced. Before reviewing the legislative provisions, it is useful to explore these contexts in greater detail.

Historical Context

Geographically separation and enormously different historical backgrounds, inevitably influence the respective legal systems of each country. Most retain some elements of indigenous laws and customs, overlaid by internationally accepted doctrines of Law.

Social Context

Observance of legal norms cannot be divorced from social context. In all countries, laws will be more readily obeyed (with less need for punitive enforcement) if they accord with established social standards. Moreover, social norms can help to define the boundaries of legality. In contract law, for example, terms may be implied according to "established business practice". The degree of candour expected in commercial negotiations may also vary, so that what is "business-like" in one place may be seen as fraudulent or misleading in another.

Political Context

Law enforcement and political context are interrelated. Laws passed by many parliaments inevitably reflect political programs or involve a compromise between various political interests, and political considerations are often involved in the way in which these laws are enforced. In some countries Stated government policy can have exactly the same effect as formally enacted legislation". This is very different from the common law tradition according to which acts of government may be challenged if beyond legislative power or *ultra vires*.

Another difference arises in the balance between public and private enforcement of legal rights. Private enforcement of intellectual property rights in many countries is difficult within existing legal structures. In US, UK, and Australia, by contrast, private civil litigation is the usual way of resolving intellectual property disputes, while police and public prosecution involvement is infrequent (Urbas 2000).

Levels of Criminality

There is also considerable divergence in the levels of activity that might be described as "cybercrime". Even in our sub-continent Korea, Japan, the Philippines and Taiwan have reported high levels of computer "hacking" and damage from computer viruses (Infowar 2001). In Vietnam, with only 0.1 per 100 of the population subscribing to Internet services, this is so far less of a problem (Vietnam Post 2001). Similar divergence in relation to estimated copyright piracy levels and associated trade losses are observable in most recent available figures compiled by the International Intellectual Property Alliance (IIPA) in association with United States Trade Representative (USTR) classifications of intellectual property protection measures in various countries.

Based on all or some of the above factors Cybercrimes have not been dealt with uniformly across the countries, or even within the country in some instances (Such as US and Australia, where we have federal and state laws. Some of the states have very stringent laws were as others donot).

Analysis

The analysis that follows is based on adequacy of laws especially w.r.t to crimes as under the Europe's Convention on Cybercrimes.

Of the roughly 150 nations in the world over 100 countries do not have penal laws for Cyber Crimes. Of the remaining a majority of them have laws, which are not adequate to address all types of Cyber Crimes.

In the early 1970s the view among nations was that for dealing with Cyber Crimes it is essential to have new Cyber Crimes specific penal laws. This assumption rested on the premise that Cyber Crime is a distinct, unitary phenomenon, a new class of anti-social activity that cannot be dealt with through the application of extant laws. As mentioned in the previous chapter late 70s and early 80s was a period when many nations legislated new computer crimes specific penal laws.

By mid-80s it was realized that Cyber Crimes actually consists of a variety of discrete conduct, some of which can be reached under traditional penal law, some of which requires the modification of traditional penal law and some of which does, indeed require the adaptation of new penal laws. Rather than being a new phenomenon, Cyber Crime is simply the exploitation of a new technology to commit traditional crimes in a new way and concededly, to engage in a limited variety of new types of criminal activities.

Indian Context – IT Act 2000

For the purpose of analysis of efficacy of computer related crime it is worthwhile to mention since both cyber crimes as well as conventional crimes result in imposition of criminal liability, therefore, each of these categories can be predicted on the basic elements that are used to impose criminal liability. In the common law countries, crime consists of four elements:

1. Culpable mental state (mens-rea)
2. Conduct (actus-reus)
3. Attendant circumstances
4. A forbidden result or harm

The offence of forgery in the physical world consists of knowingly altering a document and/or knowingly using and alter documents for the purpose of defrauding someone to impose a criminal liability of forgery, as per extant law of crimes, the state must prove:

1. Mens-rea: The perpetuator's purpose was to defraud someone or facilitate a fraud being perpetuated by someone else.
2. Actus-reus: The perpetuator knowingly altered, made, completed, executed, authenticated, issued, transferred or uttered forge writing.
3. Attendant Circumstances: The writing was altered.
4. Harm: The perpetuator used forged writing to defraud or/to help defraud someone.

In a forgery crime committed using computers one can create a false electronic document with the help of a computer or alter an electronic document stored in a computer. Analyzing this crime against the four components reveal:

1. Mens-rea: The perpetuator's purpose was to defraud someone or facilitate a fraud being perpetuated by someone else.
2. Actus-reus: The perpetuator used a computer knowingly to alter make, complete, execute, authenticate, issued or transferred a forge document.
3. Attendant circumstances: The electronic document was altered.
4. Harm: The perpetuator used forged data to defraud or to help defraud someone.

Here a computer is simply a method which forgery is carried out; an instrument that is used to alter or otherwise falsify a document. In the physical world we never had methods specific offences i.e., we never had separate offences for forgery by pen or forgery by copying machines. Thus there is no need for having a separate offence for forgery by use of computers. So long as we legally except creation of electronic documents and/or falsification of electronic documents within the generate definition of documents.

On the same lines if other conventional crimes such as burglary, criminal trespass, cheating, pornography, murders, etc.; as they are committed in physical world and now in cyber space are analyzed against the four above mentioned elements. It is observed that the traditional law can be very well applied to deal with these crimes in the cyber world by incorporating and attributing tangible status to information and services.

The Information Technology Act, 2000 has followed the approach that conducts in the cyber world, which can be effectively addressed

1. Under traditional penal laws should remain to be addressed by traditional penal law of the country.
2. Which require amendments to the traditional penal law, the law should be so amended so as to address the issue effectively (amendments to IPC IEA, BBE, RBI Act)
3. Fresh legislations be legislated for only those discrete conducts, which require the adaptation of new penal laws.

International developments:

The first comprehensive proposal for computer crime legislation was a federal bill introduced in the US Congress by Senator Ribicoff in 1977. The bill was not adopted but this pioneer proposal created awareness all round the world.

In the year 1983, O.E.C.D., appointed an expert committee to discuss computer related crimes and the need for changes in penal law. On the basis of the findings of this expert committee O.E.C.D., recommended the member countries to ensure that the penal legislations also applied to computer related crimes.

The Council of Europe appointed another expert committee and the legal issues were further discussed leading to the recommendation No.R (89) 9. The Council of Europe adapted this recommendation on September13, 1989. The recommendation recognized the transnational nature of Cyber Crimes and contained a minimum list of offences necessary for a uniform criminal policy on legislations consigning computer related crimes.

The issue of computer related crime were discussed at the

1. 13th Congress of the International Academy of comparative law in Montreal in 1990,
2. At the UN's 8th criminal conference in Havana in 1990, consequent to which the United Nations released its guidelines on computer related crimes (UN manual on prevention of computer related crimes).
3. And in the conference in Wartburg, Germany, in 1992.

The Council of Europe adapted in September 11, 1995 another recommendation concerning problems of procedural law connecting with Information technology.

In the year 1997, the hi-tech sub-group of the G-8's senior experts on transnational organized crimes developed 10 principles and a plan of action combating computer crimes. Consequent to this in March 1998 was established a 24 hour, 7-day network of experts to assist in hi-tech crime investigation. The goal was to ensure that no criminal receives safe haven anywhere in the world, and the Law Enforcement authorities have the technical ability and legal process to find criminals who abuse technologies and bring them to justice.

In the year 1997, Council of Europe decided to re-examine the whole issue of computer related crimes a fresh and it appointed a committee of experts on crime in Cyber Space (PC- CY) the same year. The objected were to identify and define new crimes, jurisdictional rights and criminal liability due to communication on the Internet. Besides, the member countries Canada, Japan, South Africa and the United States were invited to participate in the negotiations. The Convention was finally adapted in the year 2001 and as on date 34 countries are signatories to this convention.

The convention has in its preamble the following statement: "Convince that the present convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, Networks and computer data as well as the misuse of such systems, network and computer data by providing for the crimilization of such conduct as described in this convention and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

Efforts made by International law enforcement agencies include the first Interpol training seminar for investigators of computer crimes held in 1981 by Interpol thereafter Interpol has been organizing international conference on computer crimes at regular intervals the latest was the 5th conference held in the year 2002.

Brief of Penal Statutes in various countries:

For detailed relevant laws and Comparative analysis of IT Act 2000 with UK, US, Singapore Laws and the Recommendation of Europe's Convention on Cybercrimes please refer to Appendix A, B, C, D, E.

Australia: A federal legislation for computer related crimes is contained in commonwealth law crime act 1914 in part 6-A. The offences include unlawful access to data in commonwealth and other computers.

Austria: The privacy act 2000 section 10 the acts provides for penalty for unlawful access, deliberate access intentionally transmitting data in violation of data secrecy laws, fraudulent use of data, intentional deletion of data.

Belgium: Belgium adopted new articles in the criminal court on computer crimes in November 2000. The four main problems of computer fraud, hacking and sabotage have been made criminal offences.

Brazil: Law No.9093 adopted in June 2000 makes entry of false data into the information system and, unauthorized modification or alteration to the information system has criminal offences.

Canada: Canadian criminal court section 342.1 makes illegal access, unauthorized interception, and disclosure of source scores criminal offences.

Chile: Law and automated data processing crimes no.19.223 (1993) acts of illegal access, illegal use of information, unauthorized interception, unauthorized interference have been made as criminal offences.

China: The laws relating to Cyber Crimes in China are as follows:

1. Decree no.147 of the State Council of the Peoples Republic of China (1994)
2. Regulation of the People's Republic of China on protecting the safety of computer information.
3. Computer information network and internet security, protection and management regulations (1997)

Hong Kong: The telecommunication ordinance: unauthorized access to computers by telecommunication (section 27A) access to computer with criminal or dishonest intent (section.161) has been made criminal acts.

Denmark: Penal code section 263 makes unlawful access to information or programmes in a data processing system punishable.

Estonia: The Estonian criminal court makes destruction of programmes and data (section 269), computer sabotage (section 270), unauthorized use of computers, systems, networks (section 271), unauthorized interception or interference, (section-272), spreading of computer viruses (section 273), punishable.

France: The penal code (1993) makes attacks on systems for automatic data processing which include fraudulent gaining access, suppression, modification, alteration of data, hindering or distorting of functioning of automatic data processing system punishable. The act further makes the act of fraudulently suppressing or modifying data into an automatic data processing also punishable.

Germany: Penal code section 202A, which deals with data espanage, makes acts such as unauthorized access, unlawful erasure or alteration of data, punishable.

Greece: The criminal code article 370C makes unlawful access punishable.

Hungary: Computer fraud have been explicitly made a crime computer fraud committed by using an electronic card for public or mobile telephone, altering the micro program for the mobile telephone have also been made crimes.

Ireland: Unlawful access and unauthorized deletion/alteration of data are offences under the criminal damage act 1991.

Israel: The computer law of 1995, section-4, prohibits unlawful access, unlawful wire tapping to computer systems or equipments connected to such systems.

Italy: Penal code article 615 makes acts of unauthorized access into computer systems, destruction or damage to computer systems, partial or total interruption, illegal possession and diffusion of access codes to computers or telephone systems punishable.

Japan: Unauthorized computer access law no.128 of 1999 makes acts of unauthorized computer access, acts of facilitating unauthorized computer access punishable.

Latvia: The criminal law section 241 makes punishable acts of arbitrarily accessing computer systems, and bleaching of computer software.

Malaysia: Computer crimes act 1997 makes unauthorized access to a computer punishable.

Malta: Electronic commerce act chapter 426 Part-8 makes unlawful access to, or unauthorized use of information, unauthorized copying of data/software, hindering access to any data/software, impairing the operation of any system/software, disclosure of passwords, penal offences.

Mauritius: The Information Technology (miscellaneous provision act 1998) makes computer misuse illegal access, unauthorized modification or suppression of data criminal offences.

Mexico: Penal code part-9 chapter 2 makes unauthorized modification, destruction, causing loss of information contained in computer systems, unauthorized access as penal crimes.

Netherlands: Criminal code article 138A intentional/unlawful access to automated systems is penal wrongs.

New Zealand: Accessing computer systems for dishonest purpose, damaging or interfering computer systems, unauthorized access to computer systems are punishable acts under the law.

Poland: The penal code makes unauthorized access, unauthorized acquisition of information, unauthorized destruction, alteration of data, destruction/alteration of records in transit are punishable acts.

Portugal: The criminal information law of 1991 makes unauthorized access, acquiring of information as punishable acts.

Philippines: The public act no.8792 section 33 makes hacking or cracking – unauthorized access into or interference in a computer system in order to corrupt, alter, steal, or destroy data/programs, introduction of computer viruses as punishable offences.

Sweden: Penal code chapter4 section9-C, makes unlawful access to automatic data processing, unlawful alteration, eraser, insertion of data, software punishable acts. Acts of attempts and preparation are also punishable.

Switzerland: Penal code article 143 makes unauthorized access to data processing system punishable acts.

Turkey: Penal code section 525/A makes unlawful access; unlawful obtaining of programs, data or other components from an automated data processing system, unauthorized transmission/reproduction of program data or any other component within an automated data processing system with intent to cause loss as punishable acts.

The computer laws of United Kingdom, United States, Singapore and the recommendations of Council of Europe's Convention on Cyber Crimes have been studied in detail and compared with IT Act 2000. The findings are appended as annexure B,C,D,E.

Acts constituting a crime with some differences with regards to differences in legal, social, cultural traditions of a country are more or less the same in most countries. Over the years, as a result of recommendation of various conventions and committees, a uniform consensus seems to be evolving on what acts should constitute a crime and require interventions at national/international levels.

The Council of Europe's Convention on cyber crimes seeks to improve the means to prevent and suppress computer related crime by establishing a common minimum standard of relevant offences. The Convention recommendations to adopt legal legislation addressing five types of computer crimes.

1. Illegal interception of and/or interference with computer data, illegal access to and/or interference to computer systems, and the misuse of devices to commit any of these offences.
2. Computer related forgery and fraud
3. Child pornography
4. The infringement of copyrights and related rights.
5. Provisions governing the imposition of aiding and abetting corporate liability.

The convention proposed by the Centre for International Security and Co-Operation (CISAC) recommends adoption of laws prohibiting the following:

1. Illegal entry into a computer system
2. Manipulating data to functioning of a computer system and/or to cause substantial damage to persons or property.
3. Interfering with authentication or tampered deterred mechanisms
4. Manufacturing or distributing a device used to commit any offence
5. Using computer technology to engage in activity outlawed.

Both the above conventions are estimable attempts to begin the process of establishing consistency in the cyber crime laws of various nations.

Not differentiating between civil wrongs and legal wrongs (criminal offences) as stipulated by IT Act 2000, since as awareness of people in India, towards the rights and privileges increases, civil wrongs would also address the issue of infringements on personal rights effectively, a comparative study containing 10 different type of cyber crimes in 4 categories viz.,

1. Data related crimes including interception, modification and theft
2. Network related crimes including interference and sabotage
3. Crimes of access including hacking and virus distribution
4. Associated computer related crimes including aiding and abetting cyber criminals computer fraud and cyber forgery are tabulated as follows:

COMPARATIVE STUDY OF COMPUTER RELATED LAWS

Country	Data Crimes			Network Crimes		Access Crimes		Related Crimes		
	Data Interception	Data Modification	Data Theft	Network Interference	Network Sabotage	Unauthorized Access	Virus Dissemination	Aiding & Abetting	Computer-Related Forgery	Computer Related Fraud
Australia	X	X	X	X		X			X	X
Brazil		X			X	X		X		
Canada	X	X	X	X	X	X	X			X
Chile	X	X	X	X	X					
China		X	X	X			X			
Czech Republic		X	X		X	X				X
Denmark		X		X						X
Estonia		X	X	X	X	X	X	X		X
India		X	X	X	X	X	X	X	X	X
Japan	X	X	X	X	X	X		X	X	X
Malaysia		X				X		X		X
Mauritius	X	X		X	X	X	X	X	X	
Peru	X	X	X	X	X	X				X
Philippines	X	X	X	X	X	X	X	X	X	X
Poland		X	X	X				X		
Spain	X	X	X					X		X
Turkey		X	X	X	X		X	X	X	X
United Kingdom		X		X	X	X		X		
United States	X	X	X	X	X	X	X	X		X

* Crimes include civil wrongs also

Crimes / Wrongs mentioned above:

1.	Data Interception	Interception of data in transmission
2.	Data Modification	Alteration, destruction or erasing of data
3.	Data Theft	Taking or copying data, regardless of whether it is protected by other laws e.g. copyright act etc.
4.	Network Interface	Impeding or preventing access for others. (Distributed denial of service attacks, flooding web sites, or ISPs
5.	Network Sabotage	Modification or destruction of a network or system
6.	Unauthorized Access	Hacking or cracking to gain access to system or data
7.	Virus Dissemination	introduction of software damaging to systems or data
8.	Aiding and Abetting	Enabling the Commission of a Cyber crime / wrong
9.	Computer-related forgery	Alteration of data with intent to represent as authentic
10.	Computer-related Fraud	Alteration of data with intent to derive economic benefit from its misrepresentation

As is evident from above that as far as the substantial law is concerned, the situation in India is satisfactory. Data Interception Crime is proposed to be under sections 63 CCB.

Comparative Study of Procedural Laws

General

Electronic evidence and information gathering have become central issues in an increasing number of crimes and offences. Earlier electronic or computer evidence used to mean the regular printouts from a computer, but for many years, law enforcement officers have been seizing data media, computers themselves, as they have become smaller and smaller. Investigators have generated their own printouts sometimes using the original application program, sometimes specialist analytical and examinational tools. More recently, law enforcement agencies have found ways of collecting evidence from remote computers to which they do not have immediate physical access.

These procedures form part of what is now termed as computer forensics. Though at sometimes, the term also includes the use of computers to analyze complex data. Computer forensics is about evidence from computers that is sufficiently reliable to standup in court and be convincing.

The term computer forensics was coined back in 1991 in the first training session held by the International Association of Computer Specialist in Portland, Oregon. Computer science is science exercised on the behalf of law in the just resolution of confect (Thornton, 1997). Like any other forensic science computer forensics deals with the application of law to a science. In this case, the science involved is computer science and at times we find it to be referred as forensic computer science.

Computer forensics deals with the preservation, identification, extraction and documentation of computer evidence. Computer forensics has also been described as the autopsy of a computer hard disc drive using specialized software tools and techniques to analyze the various levels at which computer data is stored. Cross-validation to the use of multiple tools and techniques is standard in all forensic sciences validation to the use of multiple software tools; computer specialist and procedures help authenticate, and increase the believability of the evidence.

Some of the most important reasons for improper evidence collection are poorly written policies, lack of an established incidence response plan, incidence response training, and a broken chain of custody.

Chain of custody is the roadmap that shows how evidence was collected, analyzed and preserved in order to be presented as evidence in court. Proving that the chain of custodies unbroken is a prosecutor's primary tool in authenticating electronic evidence. Establishing a clear chain of custodies is social because electronic evidence can easily altered. A clear chain of custody demonstrates that electronic evidence is trustworthy. Preserving a chain of custody for electronic evidence at a minimum require that

1. No data has been added, changed, deleted from the seized evidence.
2. The seized evidence was duplicated exactly.
3. A reliable duplication process was used
4. All media was secure.

Types of evidence:

Indian Evidence Act as amended by the IT Act, 2000 now recognized electronic evidence also as evidence. However, all the data, which may have been collected during the course of investigation, may not be admissible as evidence in the light of law. Nations follow two different principles with respect to admissibility of evidence. Many nations (the continental law countries) operate according to the principle of free introduction and free evaluation of evidence ("systeme-de-l', in time-conviction"). Legal systems based on these principles in general do not find it difficult to introduce computer data as evidence. Problems occur only when procedural provisions provide specific regulations for the proof of judicial acts or prove with legal documents. In common law countries, (India is one of them) admissibility of evidence is to a greater extent, characterized by oral and adversarial procedures. All evidence introduced in a court of law has to stand the scrutiny of the prescribed legal process. Not all material that is collected during the course of the investigation is evidence.

As is in the case of written or oral evidence, computer evidence also be classified into 3 main categories:

1. **Material evidence:** Material evidence is any evidence that speaks for itself without relying on anything else. In digital terms, this could be a log produced by an audit function in a computer system, provided that it can be shown to be free from contamination.

2. **Testimonial evidence:** Testimonial evidence is any evidence supplied by a witness. This type of evidence is subject to the perceived reliability of the witness, but as long as the witness can be considered reliable, testimonial evidence can be almost as powerful as real evidence. Word processor documents written by a witness could be considered testimonial as long as the author is willing to depose that he wrote them.
3. **Hearsay:** Hearsay is any evidence presented by a person who is not a direct witness. Word processor documents written by someone without direct knowledge of the incident or documents whose authors cannot be traced fall in this category? Except for in special circumstances, such evidence are not admissible in court of law.

The rules of evidence:

The five properties that evidence must have apply equally to electronic evidence.

1. **Admissible:** Admissible is the basic rule (the evidence must be able to the use) in court or otherwise. Admissibility of evidence is governed on various legal requirements, which have to be complied with, and failure to complier is equivalent to not collecting the evidence in the first place.
2. **Authentic:** It has to be proved in a court of law that the digital evidence is what it purports to be and is related to the incident in question in a relevant way. Inability to prove the authenticity or relation to the incident in question would nullify the evidence.
3. **Completeness:** It is not enough to collect the evidence that shows just one perspective of the incident. It would never suffice to collect evidence that

can prove the attacker's actions only. There is also need to collect evidence to prove that others involved were innocent. For instance, if the prosecution wants to prove that the suspect was logged on to a computer system at the time of incident they also need to show who all were logged on to that computer system and why they think they did not commit that incident. This is referred to as exculpatory evidence and is an important part of proving a case.

4. **Reliable:** The evidence being presented to the court must be reliable. Evidence collection and analyzes procedure should be such that they do not cast doubt on the evidence authenticity and veracity.
5. **Believable:** The presented evidence should be clearly understandable and believable by a court of law. Presenting digital evidence as a binary dump will serve no purpose. If the digital evidence is presented in a formatted, human understandable version the prosecution has to actly prove the relationship of this formatted human understandable version to the original binary version which can be verified by a third party so that courts of law can believe them.

In view of the above law enforcement personnel's must follow the judicial procedures laid down, to ensure evidence admissible in court and should always be aware that their investigations may be contested on technical grounds. Investigations in an automated environment requires standard methods and procedures for two main reasons:

1. Evidence has to be gathered in a way that will be accepted by a court of law. This will be easier if standard procedures are formulated and followed. This

will also facilitate the exchange of evidence in cases having international ramifications especially if investigators from all countries collect evidence in a similar manner.

2. Every care must be taken to avoid doing anything, which might corrupt or add to the data, even accidentally or cause any other form of damage. The use of standard methods and procedures will diminish this risk of damage. In some cases, it is inevitable that some data will be changed or over written during the examination process. Thus there is a need for a thorough understanding of technology, which is being used for examination and also need for documentation so that it would be possible to explain the causes/effects later on in a court of law.

General Procedure:

Internationally, it is recognized that the diversity in personnel, experience and equipment available in the forensic sections of the various forensic laboratories and other law enforcement agencies throughout the world makes the task of reaching a consequences of opinion about how digital evidence is to be seized, examined using various types of technologies should be carried out is an enormous one. There is a journal consequence that a four step procedures the follow for collecting and analyzing digital evidence.

1. **Identification of evidence:** This involves distinguishing between evidence and junk data. There is a need to know what the data is, where it is located, and how it is stored. There is a need to have expertise to work out the best day to retrieve and store any evidence found.

2. **Preservation of evidence:** The evidence has to be preserved as close as possible to its original state. There is a need to document and justify any change made during this process.
3. **Analysis of evidence:** The stored evidence should be analyzed to extract the relevant information and recreate the chain of events. There is a need to have a in depth knowledge of what one is looking for and how he would get it.

Presentation of evidence: Communicating the meaning of evidence is vitally important. The manner of presentation is important and it must be understandable by court of laws. The evidence should remain technically and I legally correct and should be creditable.

The argument against legislation of fresh laws for cyber world does not hold good for the procedural laws. The new technology has necessitated the use of new techniques for investigation, search, seizure and collection of evidence and cooperation to be extended in the investigation, which cannot be addressed by the tradition criminal procedural law. The situation is not unprecedented. The advent of telephone and its use in the commission of traditional crimes led to the procedural law relating to tapping of telephone conversation and lately its admissibility as evidence under POTA Act.

Procedural Law w.r.t. Computer-related crimes in India

Certain provisions of the IT Act provide certain powers, which will be helpful to the investigating authority in the investigation of a computer-related crime.

i. **Section 69 IT Act:** Directions of Controller to a Govt. agency to intercept communication and to the subscriber to extend facilities and technical assistance to decrypt information.

ii. **Section 63 of Communications Convergence Bill 2000:** Power of Interception by an authorized officer

iii. **Section 75 IT Act:** Act to apply for offence or contravention committed outside India.

iv. **Section 76 IT Act:** Confiscation.

v. **Section 78, IT Act:** Power to investigate offences rests with officers not below the rank of a superintendent of Police

vi. **Section 79 IT Act:** Network service providers not to be liable for any third party information or data made available by him in certain cases.

vii. **Section 80 IT Act:** Power of police officer and other officers to enter, search, etc: The officer not to be below the rank of Deputy Superintendent of Police and he can search any public place without any search warrant

viii. **Section 81 IT Act:** The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.

ix. **Section 63 of proposed CCB regarding interception of communication**

x. Provisions of search and seizure as contained in CrPC, 1973 (Sec. 91, 92, 93, 94, 100, 165 etc.)

Comparison with Singapore Law:

i. Power of investigation is not limited by rank of investigating officer but delegated to Commissioner of Police, who can further authorize the officers to investigate.

ii. Power to summon assistance in decryption, code, technology etc. rests with the investigating officer.

Comparison with UK Law and Council of Europe's convention on Cyber Crime:

The Convention having taken into account the work done in this regard by the United Nations, the OECD, the European Union and the G8; Committee of Ministers Recommendations has recommended for inclusion of provisions to:

(i) Enable competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

(ii) Oblige the person in possession of the data to preserve and maintain the integrity of that data for at least 90 days at a time pending its disclosure

(iii) Ensure that expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication

(iv) Ensure the expeditious disclosure to the competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

(v) Empower competent authorities to order a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and a service provider offering its services in the territory of the competent authority to submit subscriber information {any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established

a. The type of communication service used, the technical provisions taken thereto and the period of service;

b. The subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c. Any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement} relating to such services in that service provider's possession or control.

(vi) Adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a. A computer system or part of it and computer data stored therein; and

b. A computer-data storage medium in which computer data may be stored in its territory.

(vii) To ensure that where its authorities search or similarly access a specific computer system or part of it, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.

(viii) To empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs (vi) and (vii). These measures should include the power to:

a. Seize or similarly secure a computer system or part of it or a computer-data storage medium;

b. Make and retain a copy of those computer data;

c. Maintain the integrity of the relevant stored computer data;

d. Render inaccessible or remove those computer data in the accessed computer system.

(ix) To empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs (vi) and (vii)

(x) To empower its competent authorities to:

a. Collect or record through the application of technical means on its territory, and

b. Compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means or

ii to co-operate and assist the competent authorities in the collection or recording of, traffic data (and content data in specified cases), in real-time, associated with specified communications in its territory transmitted by means of a computer system.

(xi) To adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

The recommendations if applied will provide the necessary legal back up to the investigator to face the challenge of investigation of cyber crime. Analyzing as to whether the above recommendations stand applied in Indian procedural law, it is felt that legal scenario is very hazy in respect of italicized recommendations. The gaps remain to be filled up especially in respect of obligations of ISPs, powers of Investigating Officers to request traffic data from ISPs, procedural aspects and tools (having legal sanctity such as FBI's DCS1000 in pen trap orders in USA) needed for seizure of data (in order to maintain its integrity and admissibility) real time traffic and content monitoring.

Apart from this Regulation of Investigator Powers Act, 2000 of UK is another important legislation providing for conditions and authority under which interception (including mass surveillance) of communication including traffic data can be made. It also empowers the secretary of State to require the communication providers to maintain interception capabilities (at Government cost) to give effect to interception warrants. The Act also authorizes law enforcement officers to serve written notices requiring the protected data in plain text or keys to unlock the data. Such powers relevant to law enforcement purposes are already broadly provided in section 63 of CCB.

Comparison with US Law:

The main law in USA w.r.t. interception of communication is, 18 U.S.C. § 2702, Disclosure of Contents, 18 U.S.C. § 2703. Requirements for Governmental Access and USA Patriot Act, 2001.

§ 2702: Protects the disclosure of contents of communication-by-communication service providers. Corresponding provisions can be found in the CCB, 2000 (sec. 64). However, in § 2702, there is a provision wherein the provider can disclose the contents of communication to a law enforcement agency if the contents relate to commission of a crime. Such a provision can be made in India also.

§ 2703: After obtaining a warrant, the law enforcement officer can obtain contents of stored communication upto 180 days old besides information incidental to contents of communication such as session timings, date, telephone nos. etc. Such provisions are contained in sec. 63 of CCB also. However under § 2703 there is a provision that pending the court order, the service provider will take all necessary steps to preserve evidence for a total duration of 180 days. This scheme needs to be copied verbatim in India and a duty should be cast upon all service providers to maintain transaction logs for 180 days and take measures to preserve evidence on request of law enforcement authorities pending the order from competent authority.

USA Patriot Act, 2001: The main features of this act relevant to computer related crimes are that law enforcement officers are authorized to obtain stored wire communications such as unopened voicemail, unopened MIME etc. can now be obtained from the service provider by a search warrant and wire tap order is not required. The situation in this regard in India remains ambiguous and it is unclear whether during the search of a service provider's computer, whether unopened stored wire communication can be legally accessed or it requires specific order under section 63 CCB.

The USAP Act also lists out the specific communication and user identity related details that service providers are required to maintain and which the law enforcement agencies can demand. This is a basic and urgent need of all investigating authorities and similar provision needs to be made in India also. The Act permits service providers to disclose content as well as non-content information of users' communication in certain situations such as imminent danger of death to someone. The Act also enlarges the scope of all relevant legislation concerning 'pen register and 'trap and trace devices' to include collection of non content related communication specific to use of computers such as email, ports, IP addresses etc and authorizing the courts to issue pen register and trap and trace devices order which have nationwide validity. The Act also allows victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems without the requirement of wiretap orders. Under new section 2511(2)(i), law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Similarly, the Act introduces wide-ranging amendments in the existing law to make investigations speedier, provide defense to ISPs for preservation of evidence done in good faith, enlarges the jurisdiction of court warrants to include the whole of USA in case of search warrants pertaining to email etc. However most of these amendments are specific to federal structure of US and strong element of privacy of individuals their, which is not the case in India.

For a detailed analysis on RIPA and Patriot Act please refer to the Annexure.

Recommendations:

1. There is an overlapping in the civil wrongs covered in Chapter IX (Sec. 43) and offences covered under Chapter XI of IT Act. Although, there is no element of double jeopardy in prosecuting a person for a civil wrong as well as for criminal offence, the criminal prosecution remedy should be limited by amending section 66 of IT Act to remove confusion. Such amendments can restrict the scope of application of section 66 IT Act by making it applicable to only protected systems and causing losses exceeding particular value and/or affecting particular interests such as Critical Infrastructure etc.

2. Protected systems should be defined inclusively within the act itself as in case of Singapore law.

3. Power to investigate computer related crimes should not be limited by rank but should be knowledge-specific and to be decided by Directors General of Police based on certain laid down policy such as qualification in 'computer course'. Such an approach will be on lines of Singapore law and will also obviate the present dichotomy wherein the computer-related crimes covered under IT Act can be investigated by an officer not below the rank of a DySP whereas computer related crimes covered by IPC can be investigated by any police officer.

4. There is a dichotomy in respect of applicability of the IT Act outside India vide section 75 of the Act as applicability of IPC (covering computer-related crime as per IPC scheme) is limited by section 4 of IPC. This needs to be

clarified. The whole issue of jurisdiction in transborder crimes (which need to be specified clearly) needs to be considered in a holistic manner by way of amendment in the Indian Penal Code of in the IT Act itself.

5. The present powers to order interception and decryption under the IT Act rest with the Controller. Such a power should rest with a Superintendent of Police in order to preserve volatile and perishable evidence. In order to prevent misuse of powers, control of Controller can be maintained by the requirement of ratification of the order of SP by the Controller before the information can be actually procured by the investigating authority.

   The Recommendations are as follows

   1) Mandatory preservation of subscriber data by ISPs

   2) Retention of traffic data by ISPs for a specified period in respect to all communications.

   3) Preservation of content data –

      Content data by itself is very volatile and any delay in capturing it will lead to a total loss of vital information. However, content data may include on the privacy of the person, as a balance powers to initiate preservation of data should rest in an authority, which is easily accessible both in time and distance. It could be the District Magistrate or the Supt. Of Police. The orders of the authority initiating preservation of data could be subject to a quasi-judicial review.

   4) Disclosure of content data – Powers for ordering disclosure of preserved content data should rest in a separate

administrative/quasi-judicial authority, which decides the issue based on facts and evidences made available to it.

5) The Central Government should make necessary rules subject to which such interception/monitoring can be ordered.

6. Although the issue of international cooperation in investigation of computer-related crimes is outside the scope of present study, it is recommended that establishment of a 24/7 (24 hours a day and 7 days a week) point in India with a nodal officer with powers to order real time interception of traffic or content data from any international agency will be beneficial. This will ensure that vital evidence is not lost and at the same time disclosure of captured data can be subjected to closer judicial scrutiny.

7. The section 66 of IT Act appears to cover data stored in a computer resource and not data at all stages of storage or transmission. This anomaly needs to be clarified. There is a need to adequately provide legal protection to Information in Transit, through a suitable amendment to section 66..

8. Section 100 of CrPC requires that seizure memo in respect of seized articles should be signed by atleast two independent witnesses. At the same time it is imperative that steps be taken to preserve the integrity and authenticity of the seized article. In case of digital evidence, preservation of authenticity and integrity can be achieved much better by technological means such as hashing and result of hashing can be specified in the seizure memo. The hashing technology that can be used for this purpose should be specified as a technology for seizure and authentication of Digital

Evidence in the Act as has been done in the case Certifying Rules (MD5 and SHA-1)

9. A detailed list of duties and obligations of ISPs (and other service providers) w.r.t. the infrastructure they ought to develop for assistance to law enforcement agencies need to drawn up and powers given to law enforcement agencies to get this information in an expeditious way. The records to be maintained by ISPs (such as User Name, log In time, Log out time, assigned IP address, Email Message ID with corresponding IP address and Date, Web page address with last upload time, IP address and image of the page, Verified subscriber name and address, account opening and closing dates, login ID, Email account name, domain name, static IP address, client account information such as mail box capacity, Incoming Mail server Name, message contents, message routing history etc.) and the duration for which this record is to be maintained must be clearly defined and made mandatory. The issue of allowing multiple login by ISPs also needs to be reconsidered.

10. The problem of using encryption in furtherance of crime is one, which needs to be tackled urgently. New an new technologies are emerging which help criminals to conceal / hide information in furtherance of crime.

It is recommended that

(i) Scope of Section 69 IT Act be enlarged to include all types of technologies in use for concealing information.

(ii) Possession of such tools, including other tools for committing crime be made punishable.

(iii) prohibiting unauthorized encryption (China, Russia, Saudi Arabia),

(iv) creating an offence in use of encryption in furtherance of a crime (US approach),

(v) providing mandatory key escrow (Sweden, Malaysia) and (iv) creating the power to require production of encryption keys by warrant or order by third parties (Singapore, Netherlands, Belgium, UK,).

11 Analysis of digital evidence requires a high level of skill and competence on part of the person doing so. To give credence to the findings it is necessary that people should be trained and should be legally recognized. For examination of physical documents, there exists a machinery responsible and trained for this purpose working under the office of Government Examiner of Questioned Documents.

The creation of a similar machinery is recommended, which could be called office of the **Government Examiner of Digital Evidence.**

12. Acquisition of skills and competence necessary for investigation of computer crimes depend on the attitude of the investigating officer. Officers of the same rank may have different attitudes for acquiring skills in deciding competitive environment. The Information Technology Act makes it mandatory for an officer of the rank of Deputy Superintendent of Police to investigate cases under section 78. Similarly, powers to enter, search, arrest

without warrant, rest in police officers not below the rank of DSPs under section 80. With more and more cyber cafes coming up, their increase for illegal activities increasing it may not be possible to handle the situation by law enforcement agencies because of limited of availability of officers of and above the stated ranks.

It is recommended that

i) Section 78 and Section 80 of the Information Technology Act 2000 be repealed so that provisions of Criminal Procedure Code – 1973 are applicable in such cases also.

ii) By way of orders , the Central Government may authorize conferring powers to investigate cyber crimes to subordinate officers based on their competency rather than their ranks.

13. Identity Theft, Pretext Calling, Cyber Squatting, Cyber Stalking, be made punishable wrongs (either a civil wrong or a criminal wrong)

14. Legislative responses to meet the challenges posed by Information Technology should keep pace with and should be harmonious with the various international efforts. The Council of Europe's Convention on Cyber Crimes, a detailed analysis of which is appended could serve as a model for us. The Convention recommends creation of a nodal authority to serve as a contact point for mutual assistance.

It is recommended that since the Central Bureau of Investigation is presently the nodal agency for Interpol it must also be designated as a nodal agency for investigation of computer related crimes both within as well as outside the country. However due to constitutional limitations the CBI cannot investigate into any offence in any state without the consent of the State Government concerned. Invariably information is the subject matter of cyber crime and in a networked environment information flees at the speed of light across the state and national boundaries. Even within a country it will criss-cross over many state jurisdictions. Hence in matters relating to offences committed on the internet where crimes can be remotely engineered unless there is a Central agency to deal with cyber crimes, law enforcement efforts will not meet with success. In the recently submitted Report of the Committee on Reforms of Criminal Justice System (Justice Malimath Committee Report) it is recommended that there is a need for a Federal Law to deal with crimes of inter-state and international/transnational ramifications and a suitable entry to that effect must be incorporated in the List I (Union List) of the Seventh Schedule to the Constitution. This recommendation of the Malimath Committee is a welcome recommendation and is required to be urgently given effect to fight cyber crime.

15. Law is only one of the institutions, which regulates human behaviour. Although a very important determinant in regulating human conduct, it is no means, the only one. There are other institutions as well .The family, religion, educational institutions and other groups with in the society have a vital role to play in shaping ethical values in Cyberspace.

It is felt that there is a need of educating the public and also the Internet users in particular about what constitutes a good ethical behavior on the Internet.

It is recommended that the Information Technology Act 2000 should be amended to provide that all educational institutions imparting education in computers including computer institutes should include in their curriculum or part of their training module a topic on cyber ethics.

Note: As directed by the Chairman following five recommendations were submitted to the Department of Information technology for immediate action

1. Enlarging the scope of Section 3 IPC.
1. Creation of the office of Government Examiner of Digital Evidence.
2. Disclosure of Information relating to Computer Passwords / hardware Locks.
3. Interception of Traffic and logging information by System Administrators and ISPs.
4. Definition of 'Protected' systems in the context of computers and networks.

All the above recommendations where presented by Shri Ashok Dohare before the inter-ministerial working group meeting held in the Department of Information Technology. All the recommendations were deliberated upon in a number of forums and have been accepted in principle for necessary action by way of necessary amendments.

Identification of Appropriate Technologies / Procedure for Seizure, Acquisition and Analysis of Digital Evidence.

The digital age can be characterized as the application of computer technology as a tool that enhances traditional methodologies. The incorporation of computer systems as a tool into private, commercial, educational, governmental, and other facets of modern life has improved the productivity and efficiency of these entities. In the same manner, the introduction of computers as a criminal tool has enhanced the criminal's ability to perform, hide, or otherwise aid unlawful or unethical activity. In particular, the surge of technical adeptness by the general population, coupled with anonymity, seems to encourage crimes using computer systems since there is a small chance of being prosecuted, let alone being caught. These "cyber-crimes" are not necessarily new crimes, but rather classic crimes exploiting computing power and accessibility to information. They are a consequence of excessive availability and user proficiency of computer systems in unethical hands. To catch and prosecute criminals involved with digital crime, investigators must employ consistent and well-defined forensic procedures.

Digital Forensics

Digital forensics is a relatively new science. Derived as a synonym for computer forensics, its definition has expanded to include the forensics of all digital technology. Whereas computer forensics is defined as the collection of techniques and tools used to find evidence in a computer, digital forensics has been defined as

> "the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation,

and presentation of digital evidence derived from digital sources for the purpose of facilitation or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations"

Digital forensics has become prevalent because law enforcement recognizes that modern day life includes a variety of digital devices that can be exploited for criminal activity, not just computer systems. While computer forensics tends to focus on specific methods for extracting evidence from a particular platform, digital forensics must be modeled such that it can encompass all types of digital devices, including future digital technologies. Unfortunately, there does not exist a standard or consistent digital forensic methodology, but rather a set of procedures and tools built from the experiences of law enforcement, system administrators, and hackers. Palmer suggests that the evolution of digital forensics has proceeded from ad hoc tools and techniques, rather than from the scientific community, where many of the other traditional forensic sciences have originated. This is problematic because evidence must be obtained using methods that are proven to reliably extract and analyze evidence without bias or modification.

Lack Of Digital Forensic Standarization

In many digital crimes, the procedures for accomplishing forensics are neither consistent nor standardized. A number of people have attempted to create rudimentary guidelines over the last few years, but they were written with a focus on the details of the technology and without consideration for a generalized process. For example, Farmer and Venema outline some basic steps in their Computer

Forensics Analysis Class notes. Their guidelines include steps such as "secure and isolate, record the scene, conduct a systematic search for evidence, collect and package evidence, and maintain chain of custody". While these guidelines were an appropriate foundation, the remaining portion of class notes focused on specific UNIX forensic procedures. Their definition of the forensics process as well as their ideas on specific methods for achieving each of these steps could have been abstracted to become applicable to general computer systems; however, the lack of software tools precluded the exploration of non-UNIX systems. In fact, the lack of software tools on UNIX platforms prompted Farmer and Venema to construct their own suite of tools known as The Coroner's Toolkit. These tools assist in accomplishing some of their forensic steps, primarily the systematic search for evidence. While a step in the right direction, this procedure is too focused on one platform, and not the most appropriate model for digital forensics.

Another attempt to outline a viable digital forensics process is described by Mandia and Prosise as an incident response methodology. This methodology is comprised of such steps as "pre-incident preparation, detection of incidents, initial response, response strategy formulation, duplication, investigation, security measure implementation, network monitoring, recovery, reporting, and follow-up" . No doubt a well thought out methodology, they also provide detailed directions for specific platforms such as Windows NT/2000, UNIX and Cisco Routers. Their methodology serves their intended purpose of providing the depth and breadth of investigating computer crime, and is abstract in the sense that it can be applied to general computer systems. However, since their focus is purely computer crime, they do not address the forensics process in terms of other digital devices such as personal digital assistants, peripheral devices, cell phones, or even future digital technology, computer or otherwise. Their process does begin to develop a more detailed procedure in that it addresses pre-incident preparation as an explicit step to professionally organize the forensic process prior to responding to an incident. Pre-incident preparation is the process of preparing tools and equipment, honing forensic skills and continuing to educate oneself on new technologies that might be useful in dealing with an incident.

The U.S. Department of Justice (DOJ) also attempts to describe the computer forensics process, but has intelligently realized the benefits of abstracting the process from specific technologies. This abstract process includes the phases of "collection, examination, analysis, and reporting". They do significantly better at identifying the core aspects of the forensic process and then building steps to support it, rather than becoming entangled in the details of a particular technology or methodology. This is commendable because it allows traditional physical forensic knowledge to be applied to electronic evidence. In addition, the DOJ does not make a distinction between forensics applied to computers or other electronic devices. Instead, it attempts to build a generalized process that will be applicable to most electronic devices. The DOJ also lists the types of evidence that may be found on electronic devices, potential locations it may be found, as well as the types of crime that may be associated with the evidence. For example, it lists the commonly cited hidden evidence locations such as deleted files, hidden partitions and slack space, but also lists what type of information may be stored there such as social security numbers, source code or images. This information is crosschecked against a list of suspected crimes such as identification theft, computer intrusion, or child exploitation, respectively. The identification of the types of potential evidence and the possible hiding locations on different electronic devices is a positive step for forensic practitioners to develop a generalized process that can be instantiated with a particular technology to produce meaningful results to a court of law.

Finally, the Digital Forensics Research Workshop (DFRW) is another significant participant in developing the forensics process. The unique aspect of DFRW is that it is one of the first large-scale consortiums lead by academia rather than law enforcement. This is an important distinction because it will help define and focus the direction of the scientific community towards the challenges of digital forensics. The most significant challenge is that "analytical procedures and protocols are not standardized nor do practitioners and researchers use standard terminology". The DFRW has worked to develop a forensics framework that includes such steps as "identification, preservation, collection, examination, analysis, presentation, and decision".

Forensic science is science exercised on behalf of law in the just resolution of Conflict (Thornton 1997). It is recognized that the diversity in personnel, experience and equipment available in the Forensic IT sections of various forensic science laboratories and other law enforcement agencies throughout the world makes the task of reaching a consensus of opinion about how examinations involving various types of technology should be carried out, an enormous one. Not every thing collected by law enforcement personnel in the course of investigation is evidence, in the light of law.

Nations follow two different principles with respect to admissibility of evidence. Many nations especially The Continental law countries operate according to the principle of free introduction and free evaluation of evidence ("système de l'intime-conviction"). Legal systems based on these principles in general do not find it difficult to introduce computer records as evidence.

Problems occur only when procedural provisions provide specific regulations for the proof of judicial acts or proof with legal documents however in common law countries, (India is one) admissibility of evidence is to a greater extent, characterized by an oral and adversarial procedure. Provisions of conducting search, as laid down by law / case laws can be aptly interpreted to incorporate intangible assets / computer systems. As discussed earlier, contemporary law (Criminal Procedure Code 1973), and other case laws are found wanting specially for seizing of digital evidence

Basic definitions

Evidence – any information of probative value, whether it confirms or dispels a matter asserted.

Digital Evidence – encompasses any and all digital data that can establish that a crime / civil wrong has been committed or can provide a link between a crime / civil wrong and its victim or a crime / civil wrong and its perpetrator (adapted from the definition from the definition of physical evidence by Saferstein 1998)

Digital Data – is a combination of numbers that represent information of various kinds, which include text, images, audio, and video.

Requirements of investigation in an automated environment

Law enforcement personnel must follow the judicial procedures laid down, to ensure evidence is admissible in court and should always be aware that their investigations may be contested on technical grounds.

Investigations in an automated environment require standard methods and procedures for two main reasons.

1. First of all, evidence has to be gathered in a way that will be accepted by a court of law. This will be easier if standard procedures are formulated and followed. This will also facilitate the exchange of evidence in international cases if investigators from all countries collect evidence in a similar way.
2. During the investigation of computer systems, every care must be taken avoid doing anything, which might corrupt or add to the data, even accidentally, or cause any other form of damage. The use of standard methods and procedures will diminish, the risk of damage. In some cases it is inevitable that some data will be changed or overwritten during the examination process. However any such change occurring should be researched and documented so that it will be possible to explain their effects afterwards.

GUIDES FOR COMPUTER BASED EVIDENCE (ACPO & SWDGE)

Principle 1. No action taken by police or their agents should change data held on a computer or other media, which may subsequently be relied, be relied upon in court

Principle 2. In exceptional circumstance where a person finds it necessary to access original data held on a target computer that person must be competent to do so and to give evidence explaining the relevance and the implications of their action

Principle 3. An audit trail, or other record of all processes applied to computer-based evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same results.

Principle 4. The officer in charge of the case is responsible for ensuring that the law and these principles are adhered to. This applies to the possession and access to information contained in a computer. They must be satisfied that anyone accessing the computer, or any use of a copying device, complies with the laws and principles.

Based on above, ilt is felt; that the process of acquisition and analysis of digital evidence be split up into three distinct steps, and the final tool to be developed should individually cater to these.

For the physical world, law required distinctly, first the seizure of the evidence, by law the investigating officer, and thereafter its analysis by the qualified expert.

The digital world poses a different challenge. A physical device seized does not necessarily mean the seizure of its digital content. Similiarly acquisition of physical evidence follows automatically with the seizure. This is not the case with digital evidence. Digitally seizing the evidence, and then acquiring it for investigation constitute two distinct steps. Since it is possible to make exact replicas, of digital evidence, it is an internationally accepted norm to make an exact replica of the seized evidence, and then work on the duplicated evidence. Working on the original evidence has been discouraged / prohibited by various agencies.

The three stages can thus be identified as

1. Seizure
2. Acquisition of evidence
3. Analysis of evidence

Seizure.

Though IT Act specifically stipulates that officers of the rank of DySP and above can only investigate offences under the IT Act, for all the cases where there would be need to seize digital evidence may not come under the gambit of IT Act. For such cases (offences of contraventions of IPC etc) the investigating officers would remain to be head constables, sub-inspector etc. this poses following challenges

1. Huge numbers of officers to train.
2. Low educational qualifications/ Technical Competence

Thus any tool developed for seizure of digital evidence has to be very user friendly, and technological non-intensive at the user end.

Technologies

Technologies proposed to be used.

i. **For ensuring integrity of the evidence being seized.**

Write Blocking

a. It is essential that no changes should be made while handling digital evidence. A change of a single BIT may render the whole evidence inadmissible. This can be achieved by write blocking the storage media which is intended to be seized by adopting a technology commonly referred to as "Write Block"

b. This is a technology, which ensures that nothing is written on a particular storage media that has been write blocked.

c. This technology can be implemented both through hardware, and software.

ii. **Duplicating evidence for analysis – Acquisition of Evidence**

a. It is essential and advisable that the original evidence should not be used for analysis, since digital technology permits to make exact replicas of any digital evidence. This can be done safely by making a bit stream backup.

b. This is a process by which a storage media is copied by reading each bit and then transferring it to another storage media thereby ensuring that an exact copy of the original digital evidence is prepared.

c. Bit-stream imaging differs from copying in that copying applies to data that is not deleted and whose location is recorded in the FAT whereas, bit-stream imaging captures and copies all data on a disk including deleted files, swap files, slack space, FAT unallocated space and FAT un-addressed space. Bit-stream backup is a mirror image of the copied disk, with the same hash value.

iii. **For Authentication and Seizure of Evidence**

Mathematical Hashing:

Mathematical hashing is equivalent to one-way encryption. The digital evidence, which at the lowest level translates into a big numerical number, is encrypted using an algorithm so that it results into a new number of a fixed length called the message digest. The hashing algorithm has some unique characteristics, which are as follows:

i. **Message digest always of a fixed length:** The digital evidence may be of any size, but on application of the hash algorithm the resulted message digest would always be of a fixed length.

ii. **Message digest is a random generated number:** The message digest is a randomly generated number. However, if the contents of the digital evidence remain the same, the hash algorithm will generate the same message digest every time it is applied on the digital evidence. This property is useful in authenticating seized digital evidence before a court of law. If application of hash algorithm on digital evidence in a court of law results in the same message digest as was obtained during the time of seizure, it indicates that the presented evidence is the same as what was seized.

iii. **One-way hash function:** It is computationally infeasible to determine the contents of the digital evidence if somebody knows the message digest. Hash algorithm is a one-way function. This property is of great importance from the legal point of view, since it prevents manipulation of digital evidence as no one can predict the message digest that would be generated once evidence has been manipulated.

iv. **Collusion free hash:** The odd that two digital evidences with different contents have the same message digest is roughly 2^{128} (i.e., 34 followed by 37 zeros). This property has two advantages:

   a. Each digital evidence can be seized uniquely by specifying its message digest.

   b. If two digital evidences have the same message digest, there is a reasonable certainty that their contents match exactly.

Limitations

By comparison of the message digest generated with the message digest generated at an earlier date of the same document can authenticate the integrity of that document if both are the same. However if the two messages do not match, it is impossible to determine what has changed.

This poses a problem in using Hash algorithms for authenticated large storage devices. A alteration even in a single bit would result in a different message digest, thereby rendering the whole evidence unbelievable in a court of law. Thus it is essential to divide the large storage devices in to smaller blocks so that even if one block gets altered all the evidence is not rendered useless. This concept of splitting larger storage devices into blocks has been implemented in the developed software Cybercheck.

Cyclical Redundancy Checksum (CRC):

The CRC is a variation of standard checksum. The advantage of the CRC is that it is order sensitive. The odds that two different digital evidences will produce the same CRC are roughly 1 in 4 billion.

However, CRC values can be reverse engineered meaning that it is possible, though difficult, to force the CRC value of one digital evidence to match that of another by altering non-printing characters within the digital evidence. For this reason, the method of choice for digital evidence authentication is the hash.

Seizure

Two technologies are presently available for seizure of digital evidence

1. CRC
2. Hash (MD5)

The odds that two different data blocks will produce the same CRC are roughly 1 in 4 billion, however CRC values can be reversed engineered. For this reason the preferred technology for digital evidence seizure is recommended to be hashing

NTI Tools offer following softwares for seizure of evidence

CRCMd5 – CRC program that validates the contents of one or more files

DiskSig – A CRC program that validates Mirror Image backup accuracy

Procedures

Steps

1. Determine if the computer is on?
    a. If yes, using a password recovery software on a diskette, recover all passwords stored in the computer (similar to 'Icain' - a freeware)
        i. Is it a standard configuration computer?
            1. If yes, determine the processes running?
                a. Make a note of all processes running and if possible take a photograph of the monitor
            2. Assess reliability of the operating system and the suspect
                a. If reliable, determine the boot sequence of the system ensuring it boots from the a: drive and then shut down in the normal mode
                    i. Whenever prompted for saving, click on 'cancel' (for Windows) and using 'Save As' command (Windows), save on a removable authenticated disk and never on the hard disk
                b. If not, pull the power cord from the system and not from the power plug
        ii. If not a standard configuration, pull the power cord from the system and not from the power plug

If computer was found switched off, carefully check for power connections & ensure that power supply is not on.

The suspect computer after this procedure is switched off, which is similar to an initial situation where the suspect' s computer on arrival of the investigating officer was not switched on.

It would be legally sound to write as much details about the Seized computer or its storage mechanism in the seizure memo itself so that uniqueness of the seized material can be established in a court of law during trial. This necessitates restarting of the suspect computer. The procedure recommended is as follows:

1. Open the system, and disconnect the power supply to all the hard drives
2. Ensure all external drives are empty.
3. Place a authenticated, write protected bootable floppy drive, which should contain
    a. Basic MS DOS system files
    b. Write blocker software program
    c. Hashing tool
    d. Password recovery tool
4. Restart the computer
5. If Computer restarts
    a. Ensure, it boots from the authenticated floppy only
        i. Immediately on turning on the computer appropriate keys should be pressed and CMOS BIOS be accessed to ensure computer boots first from the floppy.
        ii. Record the system time & date
        iii. Check for the MAC address and other CPU details, which should also be documented

iv. Make appropriate changes in the booting sequence if required so as to ensure it boots for the authenticated boot drive.

v. Save changes and Exit CMOS BIOS and let computer boot from the diskette

6. Shut down the system, pull out the power cord, and reconnect the power supply to the hard drives & restart
    a. The floppy should write protect the suspect computer's drives by running the write blocker program
    b. Determine the drive geometry which should be documented
    c. Calculate the Hash value of drive/ drives
    d. Prepare a seizure memo mentioning the message digest, as per provisions of Cr.P.C. and should be got signed as per legal requirements
    e. Decide whether the computer can be transported to the lab or not?
        i. If no, ensure security of the system till a computer forensic expert arrives for making a digital copy of the drives
        ii. If yes, shut down the computer
7. If the computer does not restart
    a. Record the fact, which should be recorded in the seizure memo
8. Pull out the cord from the computer and not from the power source

Document and label the configuration pack it securely and send to lab for investigation

Acquisition of Evidence

Globally accepted technology is making a bit-stream backup of the seized evidence, in a non-invasive manner. The implementation part differs with different products.

Safeback:

Developed (marketed by New Technology Inc.) by Chuck Guzis, for law enforcement agencies, is a law enforcement standard. It copies and preserves all data contained on the hard disk. It even goes so far as to circumvent attempts made to hide data in bad clusters, and even in sectors with invalid CRCs. Our aim should be to develop such a tool, with SAFEBACK as a benchmark.

EnCASE :

Marketed by Guidance Software Inc, it makes a bit-stream backup, however the copied file is compressed using a patented algorithm. The advantage is that the duplicated file is much smaller than the original, making it possible to use a same size storage media for making copies. The duplicated evidence is stored in the form of a file, which can be later on analyzed.

EnCase provides an option of preview of the evidence, in a non-invasive manner, before acquisition, so that only relevant information/evidence may be seized, thus saving time & energy.

Expert Witness:

Expert witness is non-invasive to the original computer. It uses a wizard interface for acquisition of data. The investigating officer walks through a series of simple steps and uses the responses and information provided by the user to create a case profile, thereby reducing chances of mistakes and ensuring establishment of a chain of custody.

Provides an option for either compressing the duplicated image or copying it without compression.

iLOOK:

Makes a Bit-stream backup, distributed free of cost to law enforcement personnel. It has capability to analyze evidence acquired through other commercially available software.

DIBS:

DIBS (Data Image Backup System) is an integrated acquisition and analysis tool. It uses a unique and patented technology for acquisition of Digital Image called DIVA (Digital Integrity Verification and Authentication protocol). DIBS copies a media onto 5.2 Gb optical re-writeable disks, maintaining the disk geometry.

In each cartridge is a reference area, which contains copy specific information – such as CPU type and speed, hardware equipment indicators, copy drive serial number, cartridge sequence number, exhibit details, unique password, and real date and time as entered by the operator. A pre-specified area of each cartridge is set aside to store integrity verification information for each block.

The evidence being copied is divided into blocks. As each block is copied and verified, a hash value is generated and stored on the cartridge, and copying proceeds to the next block. Each block is treated in this fashion. Once the cartridge is full, a single hash value of all the hash values is calculated and encrypted and stored in the pre-designated area of the cartridge in encrypted text. This hash value is stored in the memory and operator is prompted to insert a new cartridge until the copy is completed. The final cartridge besides having similar information will have the accumulated value of hash of all other cartridges in the series. Once the final cartridge has been copied the operator is prompted to insert a preformatted floppy disk into the drive used to start DIBS process. All of the accumulated hash values are then written to a floppy disk together with the reference details of the whole copy procedure. Two such copies are made. One kept by the investigator and the other by the suspect.

The procedure has following advantages

1. Corrupted block can be identified and hence all evidence is not lost, if a portion or one block gets corrupted.
2. Suspect disk details help in authentication of evidence.
3. Use of optical media, helps extend the life of evidence.

RAIDS:

It is a patented hardware and software of the DIBS USA Inc.; Use of all the above software for making a bit-stream image involved an interface of a computer. Since computers have their own input devices there exists a probability of corrupting the bit-stream back-up. This hardware has no input device and hence, the possibility of introduction of errors while a bit-stream copy is being made is eliminated. The hardware is totally portable and has a printer, to which at the end of the process of making a bit-stream backup it prints a report. It is strongly recommended that attempts may be made for developing a similar tool for law enforcement agencies in India.

Various scenarios for Acquisition of Evidence:

The following four main scenarios may exist while attempting to acquire evidence.

1. **Parallel port cable acquisition**

   A suspect computer is seized and brought to the laboratory. The suspect computer media drives are write blocked and then is booted to the acquisition tool for DOS. The computer forensic workstation is booted to windows and evidence is acquired to a parallel port.

   This process is the slowest.

2. **Drive to Drive Acquisition (in the laboratory)**

   The suspect IDE Hard drive is removed from the suspect computer and is placed in the computer forensic workstation so that both the suspect drive and the evidence IDE drive are on the same motherboard.

   A SCSI Card could also be interfaced to speed up the process, of acquisition (as in FASTBLOC). The whole process can then be completed in a purely DOS environment.

3. **Drive to Drive Acquisition (at the scene of crime)**

   In all occasion it may not be possible to shift the suspect computer or the media drive to the laboratory. The problem could be further aggravated if situation so required that the suspect media has to be acquired in its own working environment. This would necessitate plugging in the evidence media drive in the motherboard of the suspect computer and then making a bit-stream backup. The process may require imaging in the environment of the suspect computer or in a DOS environment.

4. **Network cable acquisition:**

This scenario may arise when it is not possible to remove the suspect computer or media drive since it is on the network and any removal may disrupt the working of the network. This scenario is beyond the preview of the research project and has not been examined. But it is strongly felt that any acquisition tool developed should have the capability of acquiring evidence in real time on a suspect network computer.

Recommendations for Acquisition:

The stages of seizure and acquisition have been separated solely keeping in mind the technical competence of user (sub-inspectors, equivalent and lower ranks in the law enforcement departments). Both the processes require use of Hash Algorithm on the whole storage media, which is very time consuming. And applying it twice once during seizure and again during acquisition is doubling the time required. We would have to live with it till technology by itself percolates to the end user presenting itself in a very friendly interface. It would be a future endeavor to complete both the processes simultaneously but as on date, the demand is that these two operations should be separated. Integration of the above two tools could take place in the future. But, as an implementation strategy the first few versions of the tools, should be two distinct entities.

To start with, it would suffice that the seizure tool hashes the whole disc and returns the hash value, which is noted on the seizure memo and the storage media is deemed to have been seized as per law. However, the protocol adapted by DIBS Inc., should be adopted and the tool should confer to that procedure.

The **seizure and acquisition tool** should consists of following:

1. Write protect software – for write protecting all media drives
2. A bootable software
3. Essential components of DOS
4. Hash Algorithm
5. Computer detail and disc detail extraction tool.

The capabilities of the seizure tool should include that when the investigating officer reboots the suspect computer, which he intends to seize the tool, should write block all the media drives and extract the following information:

1. Details of the CPU and configuration
2. Computers date and time
3. Storage media serial numbers

The above information should be stored in memory and thereafter the Investigating officer should be prompted to enter information like investigators name, case number, actual date and time of seizure, etc., which again should be stored in memory.

On being required to seize, the tool should start the application of hash algorithm, which should be applied on the disc after dividing it into convenient blocks depending on the size of the hard drive. Separate hash values for each block should be calculated, and encrypted and stored in memory. On completion of application of hash algorithm on all the blocks, the tool should calculate

i) The hash value of the whole disc and

ii) another hash value of the hash values calculated for each block. This set of hash values should be displayed on the monitor wherein the investigating officer brings on record the net hash value of the disc and the hash value calculated for the group of hash values of each block on the physical seizure memo. The tool should prompt the investigating officer to remove the bootable floppy and insert a fresh pre-formatted floppy wherein all these values

1. Encrypted Hash values of each block
2. Hash value calculated for the set of hash values of each block.
3. Hash value of the total storage media.
4. Case details, based on the information provided by the investigating officer
5. Details of computer hardware including storage media serial number.

are stored. The Investigating officer could make four of such copies and handover one to the suspect and obtain the receipt. The second copy is sealed with the other sealed items and forwarded to the computer forensic laboratory for examination. The third copy is kept on record and the fourth copy is submitted to the court either immediately with the intimation of seizure or as and when required by the court.

Acquisition:

What are received in the forensic lab would be the suspect storage media (either the whole computer or just the media), and a floppy drive having information as above for each of the storage media. The acquisition officer having decided on the best process for acquisition of evidence, verifies the information pertaining to media storage number, CPU number, etc., as stored in the floppy drive or on the seizure memo and thereafter on authentication, starts taking a bit-stream backup

At each stage, the generated hash values are compared with the hash values generated for the corresponding blocks during seizure so that acquisition of evidence is authenticated at each stage.

Any deviation observed is recorded and intimated to the investigating officer. The advantage of the procedure is that in the event of any block getting tampered or altered, all the evidence on the hard disc is not legally lost. On successful making of a bit-stream copy, which means all the hash values of the duplicated evidence match with the hash values, generated during seizure. The duplicated evidence is ready for examination. In case there are discrepancies, the fact is brought on record and only those portions of the evidence should be analyzed which return same hash values as were generated during seizure.

Note: Please see the appendix for the specifications for a bit-stream back-up tool, and a write-block tool.

Analysis of Evidence:

This could be most time consuming stage where the results would depend not only on the availability and quality of tools but also on the analytical capabilities of the expert.

New technologies incorporated markets large number of tools for analysis of digital evidence. They are the most authentic ones. However, most of the tools are DOS based and hence their use requires a lot of training and knowledge of computers. Some of the major tools are described below which also suggests what all capabilities should a digital evidence analysis tool have.

1. **Ana Disc:** This tool works at a very low level just requiring the bios for operation. The tool analyses a storage media and even detects extra sectors or tracks created to hide data. It is also able to read data when it has been written to unformatted diskettes.
2. **P-Table:** A programme, which identifies partition tables and operating systems in use on a hard disc drive.
3. **GetFree:** An ambient data collection tool used to capture unallocated space.
4. **GetSlack:** An ambient data collection tool for capturing files slack.
5. **Get Swap:** A forensic utility that is used to capture static swap and page files for analysis.
6. **Text Search Plus:** A text search utility used to locate key strings of text and graphic files.

7. **FileList:** A disc-cataloguing tool used to revaluate computer used time lines.
8. **Get Names:** It automatically identifies and lists English names found on computer media. Integration of this facility in the tool being developed would require developing a database of common Indian names.
9. **Get HTML:** A filtering tool that automatically identifies and reconstructs HTML documents and files relating to Internet investigations.
10. **Get GIF:** A filtering tool that automatically identifies and reconstructs GIF files.
11. **HexSearch:** A forensic hex search utility useful in finding binary data patterns associated with file header and foreign language data patterns.
12. **Seized:** A very useful programme, which is used to lock and secure evidence computers. Such a programme is essential since it protects a computer being used for analysis from being accidentally handled by an authorized people.

Most of the commercially available computer forensic utilities have all the above capabilities, which have been integrated in one suite having a very user-friendly interface. The above capabilities have been so integrated that the process of analysis is made easy.

EnCASE: This is one of the most sort of forensic utility software. Some of the unique features are:

1. The software has the capability of identifying and listing system files and other files separately. This utility helps the user save lot of time by not searching the system files. The EnCASE has a databank of the hash values of known system files. All the files on a hard disc are hashed and those files whose hash value matches with the hash values in the database are presumed to be system files and are shown separately.
2. The software has the capability of reconstructing images, in the selected folders/files and displaying them.
3. The software has the capability of graphically depicting the timelines of a selected file which include data of creation, access, modification, etc.,
4. The software is capable of generating a report at the end of the analysis.
5. EnCASE version 4 provides support for foreign languages i.e., it is fully compatible with the 16-bit Unicode.
6. It provides EnScript support also. An EnScript is a programming language consistent with C++ and Java Script. It provides powerful tools for automating complex and /or repetitive operations. This allows investigators to develop incident specific utilities tailor made for specific analysis.
7. EnCASE supports viewing of compound files such as registry files, OLE files, e-mail files (PST and DBX files).

<u>Expert Witness:</u>

A software with similar capabilities of EnCASE, but with a much better user-friendly front end. It graphically depicts the media under analysis displaying each sector as a square. It displays using different colors. The whole disc has volume boot, FAT, root folder, unallocated space, bad sectors, allocated sectors, selected files, lost cluster, deleted files, boot sector, wasted area, unused area, unknown, volume slack. This utility (volume bitmap view) is of immense help as it gives a detailed overview of the physical layout of any selected volume to the investigator.

ILOOK:

This software has been developed by Law Enforcement officer named Elliott Spencer and the software is made available free of cost to law enforcement agencies. ILOOK is a very versatile software and can be used to examine bit-stream images obtained from any forensic imaging system that creates a straight sector dump of the imaged media. Most of the commercially available softwares produce images in this format only. ILOOK can be used to examine evidence acquired through safeback EnCASE, ISO and CIF CD images, VMWare virtual discs and ILOOK image for files.

1. This software combines all the utilities of EnCASE and expert witness.
2. This software provides the feature wherein hash sets can be imported from outside to enable the software tool recognized more and more system files.
3. It supports the volume bitmap view.
4. Supports comprehensive scripting languages, compiler and runtime engine.
5. Integrated thumb nail viewer for all files of any selected volume.

DIBS:

The features of DIBS for analysis purposes are similar to that of EnCASE.

DIBS comes with a special utility software called **QuickView** Plus. This software reads a file by reading its contents rather than reading its extension. This utility is of immense help because of following two reasons:

1. The file extensions may have been intentionally altered to conceal information or deceive the investigator.
2. As an integrated package if this tool is in hand there is no need for buying compatible softwares for different files etc.,

An **Analysis tool** to be developed should have

1. Non-invasive preview of the contents of a drive.
2. Map the disc geometry, identify partitions, and list the file structure.
3. Generate or import customs sets of file hashes to enable identification of systems and other utility files.
4. Sort files by different criteria including time maps.
5. Browse basic file system, artifacts such as swap files, file slack, print spool files, files located in the recycle bin, ram slack, unallocated space, bad clusters, and erased files.
6. Support viewing of compound files including PST files support for MS Outlook.

7. Capability to open files without reading the file extensions.
8. Search and analyze media without changing the file contents, time stamps, or hash value.
9. Conduct key word search and highlight the hits and capability to archive them.
10. View all relevant time stamps of files.
11. Capability to bookmark files of interests, file segments, or images.
12. Capability to identify all graphic files, displaying them with capability of being bookmarked.
13. E-Script macro language capability for writing specific filters and programmes.
14. 16-bit Unicode compatibility (foreign language support)
15. Capability of restoring deleted evidence.
16. Stitching capabilities for information in lost clusters.
17. Archiving evidence and report generation.
18. Graphical map (volume bitmap view) showing disc allocation by cluster or sector including the layout of any file in the case.
19. Hex/text viewer showing the contents of any file (file slack to be displayed in different color).
20. Formatted reports that show the contents of the case, dates, times and investigator involved.

Recommendations:

A tool having all the above capabilities of seizure, acquisition and analysis will have to be developed in phases. A basic tool to start with should be able to execute the four requirements like reading the discs, identifying the partitions, search and analyzes of the media, extraction of the graphic files, extraction of slack space, unallocated space, deleted files, etc.,

In the second stage, functionalities like compatibility with 16-bit Unicode (foreign language support, volume bit map, etc., can be added upon).

Note: **Please see Appendix for user specifications of the seizure, acquisition and the analysis tool.**

A Working Strategy

Investigations in automated environments should be completed in three stages:

1. **Pre-investigation**

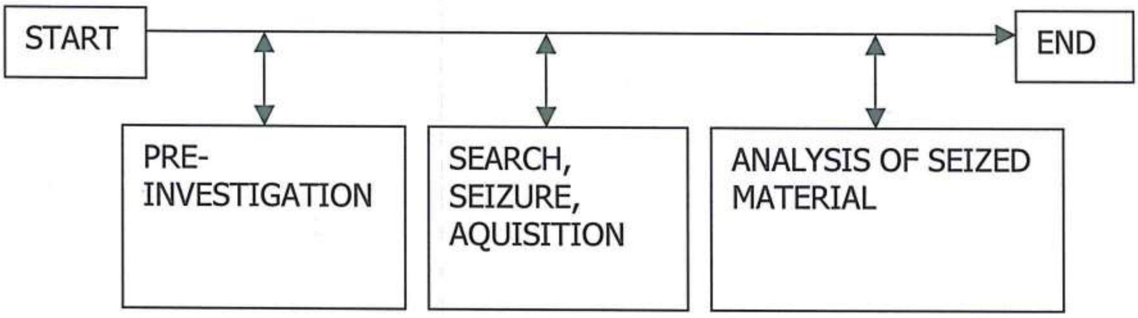
   During this stage, it is essential to collect as much information as possible about the environment under investigation. This will also help in the choice of equipment or specialists during the subsequent stages of the investigation.

2. **Searches and Seizure (and Acquisition)**

   This is the stage of the investigation when evidence is collected. Very often there is only one opportunity and there may not be a second chance. Search and there after seizure has to be conducted in such a way so that procedures followed & evidence seized is as per law.

3. **Analysis of Seized Material**

   Not only does the necessary evidence have to be extracted from the seized material, but also the operation has to be carried out in such a way that the evidence will be admissible.



Pre-investigation

Preparation for search and seizure

Collection of information

i. What is expected?

ii. Who should be present?

iii. What is to be carried?

Briefing of personnel

i. Role

ii. Authority

iii. Hindrance expected?

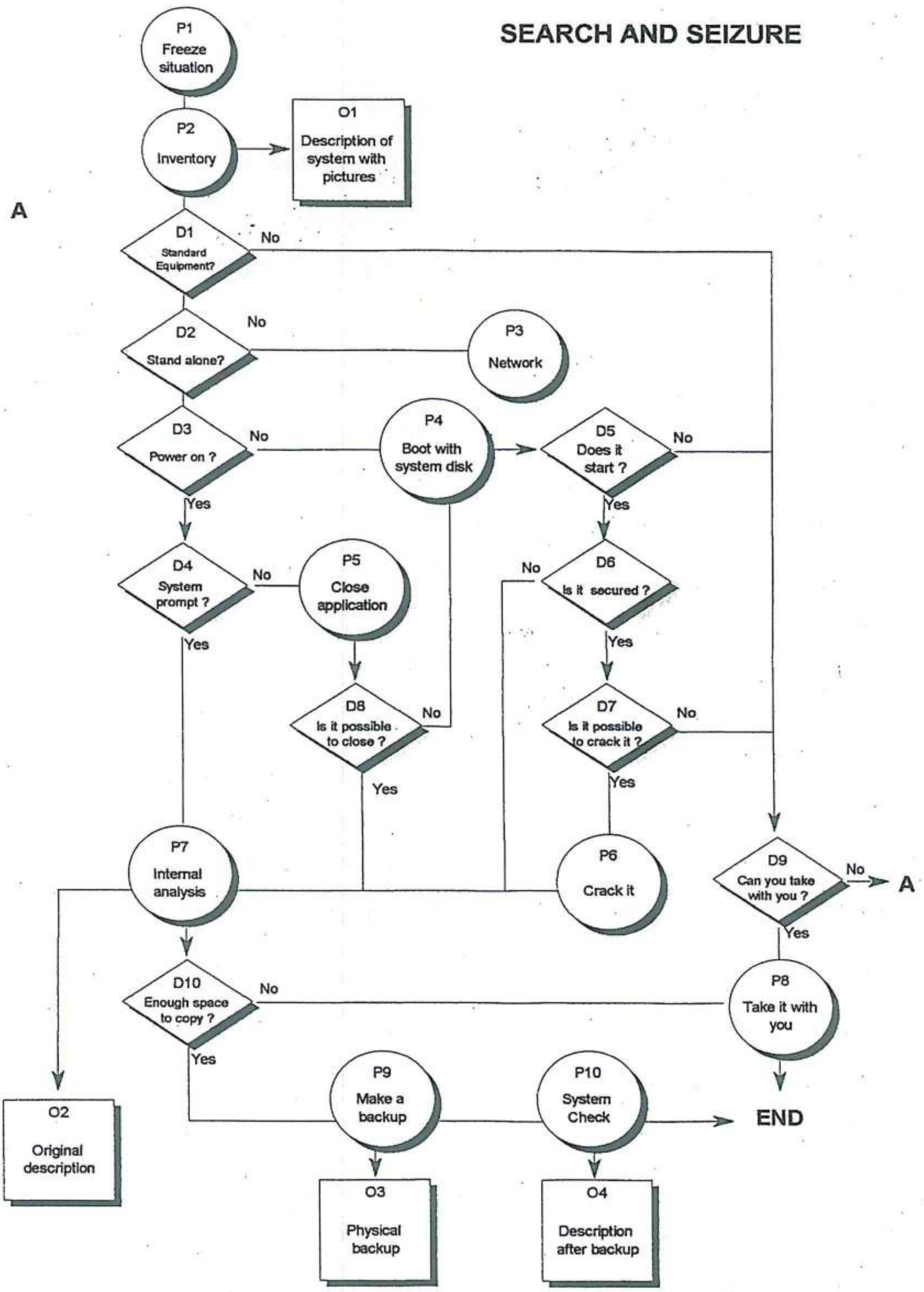
iv. What all to be searched & seized?

   a. Include other electronic storage data?

v. How to search / seize?

   a. Careless handling may destroy data?

Search and Seizure and Acquisition – flow Chart



Brief about flow chart

P1 : Freeze the situation :

1. Isolate staff
2. No changes / removal from the environment
3. Locate identify the owner / system administrator
4. Photograph / video
5. Prevent evidence destruction / transfer through data communication channels.

P2 : Inventory

1. External documented inventory of computer system and its components

O1 : Description of system

1. Physical sketch
2. Photographs

D1 : Standard equipment

1. Non standard equipments – Seize, Search at site may be risky
2. Make note of special hardware – dongles / keys

D2 : Stand-alone Computers

1. Computers could be connected by other means than cables / modems

D3 : Power on

1. Blank screen does not indicate power is off

D4 : System Prompt

1. Check whether system is in "command line mode" or if an application is running.
2. Non-recognizable prompt – decide if it is a standard equipment.

P7 : Internal Analysis

1. Aim :
   a. Is it possible to make a back up?
   b. What are the files required?
2. Analysis of hardware
   a. Check connections to ports
   b. Partitions
3. Inventory of software
   a. System date / time
   b. Size of files
   c. Hidden files / directories
   d. Directories present

O2 : Original Description

1. Full and complete description of computer
2. In - conformity with O1 & O3 & O4
3. Make sure that P4, P5, P6 have not altered the contents of the hard disk.

D10 : Enough space

1. Information from P7 is important

2. Use an adequate sized backup media

P9 : Make a back up

1. Decide type of backup required
   a. Image backup
   b. File to File backup
2. Decide on backup media
   a. Direct accessible – HDD, CD-Rom, WORM
   b. Not Directly accessible

O3 : Physical backup

1. Use of certified software & Authenticated Tools

P10 : System check

1. Second check after making the backup
   a. Check for changes in date / time / file attributes

O4 : Description after backup

1. Compare with O2 & P10

D1 : Non – standard System

1. Seize the system
2. Take expert assistance

P8 : Take it with you

1. Labeling evidence & storage

2. Protect data carriers

D2 : Not stand-alone

1. Not within the study limits

P3 : Network

1. Outside the preview

D3 : Power not on

1. Detailed note annexed

P4 : Boot with disk

1. Detailed note annexed

D5 : Does it start?

1. Check cable & power plug
    a. Refer to D9 – take it with you

D6 : Is it secured?

1. Protect devices range from simple hardware locking to software devices
    a. Contain password protection / encryption
    b. Careless shutting down may shut down the computer for ever
2. No protection devices proceed to P7

D7 : Is it possible to crack?

1. Decide where to crack? Scene of crime or in laboratory

P6 : Crack it

1. Ideal to do it in the lab under expert guidance

D4 : No system prompt

1. System running an application
2. Adopt all precautions to shut down the application

P5 : Closing Application

1. Give suspect an opportunity to comment
    a. Do not believe him blindly
2. If not possible or in doubt how to shut down the application
    a. Re-boot the system
        i. Effectively means shutting down the computer – loss of data
        ii. Re-starting may be a problem - password / hardware locks
        iii. No decision in haste

Choosing a Strategy

Pulling of the cord, one of the oldest strategies may not be the most appropriate one, especially due to advancements in technology.

Advantages :

1. Low level of expertise required
2. No alteration of data stored on magnetic disc
3. Investigation can be done by experts in labs

Disadvantages

1. Loss of volatile data
2. Hard disk may crash
3. Not advisable for large systems
4. If the computer system is password / hardware protected, restarting may be a problem
5. Making a legally valid seizure memo may be a problem
6. Delay in investigation

Various strategies available

1. Examining the suspect system using the software on the suspect system without verifying the software
    a. Advantages
        i. Requires least amount of preparation
        ii. Allows examination of volatile information
    b. Disadvantages
        i. Least reliable
2. Verify the software on the suspect's system and use this verified software to conduct investigation
    a. Advantages
        i. Minimum preparation
        ii. Allows examination of volatile information
    b. Disadvantages
        i. Requirement of many tools to verify integrity-may not be always available
        ii. Write protecting hard disk may not be possible
        iii. Getting hash values for seizure may not be possible

3. Examine the system using external media with verified software on it
    a. Advantages
        i. Convenient and quick
        ii. Allows examination of volatile information
    b. Disadvantages
        i. If a kernel is compromised, results may be misleading
        ii. External media may not have every necessary utility

4. Build a new system containing an image of the suspect system and examine it
    a. Advantages
        i. Completely replicates operational environment of suspect computer
        ii. No risk of changing its information
    b. Disadvantages
        i. Requires availability of identical hardware
        ii. Loss of volatile information
        iii. May not be cost effective solution for petty offences

All the above four strategies are not recommended since they require a very high level of expertise on the part of the investigating officer which in the context of Indian scenario would be very difficult to impart since the target officers are of the level of the Sub Inspectors.

5. Boot the system using a verified, write protected floppy disk or CD with kernel and tools

a. Advantages

   i. Convenient and quick

   ii. Evidence is defensible if suspect drives are made write protected/read only

   iii. Is the only option where suspect's computer can not be transported/ removed

b. Disadvantages

   i. Requires shutting down of suspect's computer before examination

   ii. Assumes that hardware has not been compromised

   iii. Loss of volatile information

   iv. The investigating officer has to be technically qualified in computers

6. Use a dedicated forensic workstation to examine a write protected hard drive or image of suspect's hard drive

   a. Advantages

      i. Since the investigating officer has to only shut down the computer and seize the equipment, very less expertise is required

      ii. No concern for validity of either the software or hardware on the suspect host

      iii. Evidence acquired can be easily defended in court

   b. Disadvantages

      i. Requires shutting down of suspect's computer

      ii. Loss of volatile information

      iii. Inconvenient and time consuming

Though the above two strategies may result in loss of volatile information, since they afford a simple and reliable procedure, could be adopted.

Based on the above an extraction tool which supports the following procedure is recommended for being developed.

Recommended Procedure

Basics of the recommended procedure

The proposed procedure for seizure, acquisition and analysis of digital evidence during investigation of computer related crimes is based primarily on the study of various models enumerated above, ensuring that it adequately addresses the various legal provisions of various enactments of the land.

The procedure recommended can be summarized as follows

1. **Identification:** This step is not explicitly within the field of forensics. It is essential that the law enforcement official is able to identify that an act or omission has been committed which authorizes him legally to intervene, and initiate an legal process.
2. **Preparation:** This step is also more of an administrative or legal-administrative issue, such as constitution of search and seizure teams, or obtaining of required search warrants.
3. **Strategy Formulation:** this step encompasses planning and preparation for conducting approaching a scene of crime and conduction search and seizure.
4. Seizure of evidence.
5. Acquisition of evidence and Authentication.
6. **Examination and Analysis.**
7. **Presentation of report.**
8. **Return of evidence :** as the case may be to the owner.

Steps as enumerated at serial number 4, 5, 6 being the core issues in Computer Forensics have been dealt in details in this work.

The Procedure

Limitations

This procedure applies only for a stand-alone Personal Computer, including networked computers, which have been disconnected from the network working in Windows environment,

The procedure limits itself to Disk Forensics, i.e. information stored on a storage device and not for information in transit such as in case of Internet.

Preliminary

As per section of IT Act, 2000, only police officers and above the rank of Deputy Superintendents of Police can only investigate offences under the IT Act. However, electronic evidence may be relevant in ordinary IPC crimes also. Therefore, whenever any section of IT Act, 2000 is invoked in the FIR, no police officer below the rank of a Deputy Supt. of Police shall investigate the case nor conduct any searches involving computers.

Any crime involves collection of evidence to link crime, crime scene and the criminal to one-another. Hence, in the investigation of a Computer-related crime, firstly it has to be ensured that there is an involvement of a particular computer in the crime. This could be done by investigation based on available information leading to involvement of computers. While in cases where computer is the target, it could be obvious. However, in cases where computer is used as a tool for committing a crime (such as ransom note through email, pornography etc.), this would have to be established through preliminary investigation conducted in the conventional manner..

The process of seizure of data outlined below takes into account the requirements of procedural formalities as outlined in Criminal Procedure Code as well as other well established principles of Authenticity, completeness, reliability and chain of custody of evidence.

The following terms may be construed as defined below

i. **Seize:** The process of generating a unique identity (Message Digest) of the digital evidence in a write block, and trusted environment, which is thereafter taken in the custody of the law enforcement official for the purpose of investigation.

ii. **Acquisition:** The process of making an bit-stream image of the digital evidence proposed to be seized in an write block and trusted environment. The process is deemed to be successfully completed if the message digest of the original digital evidence being seized matches with the message digest of the bit stream backup copy made on a forensically sterile storage media.

iii. **Seizure and Acquisition** – The process of simultaneously generating a message digest and a bit-stream backup of the digital evidence proposed to be seized in an write block and trusted environment. The process is deemed to be successfully completed if the message digest of the original digital evidence being seized matches with the message digest of the bit stream backup copy made on a forensically sterile storage media.

iv. **Stand Alone Personal Computer:** A Computer not connected with any network at the relevant time.

Pre-search and Seizure stage

The equipment containing the digital evidence may be contraband, a fruit of the crime, a tool of the offense, or merely a storage container holding evidence of the offense. Computers and related evidence range from the mainframe computer to the pocket-sized personal data assistant to the floppy diskette, CD or the smallest electronic chip device. Images, audio, text and other data on these media are easily altered or destroyed. It is imperative that you recognize, protect, seize and search such devices in accordance with applicable statutes, policies and best practices and guidelines.

Always keep in mind the basics

i. Electronic evidence is extremely volatile and is easily altered.

ii. Every effort should be made not to alter any electronic evidence being seized.

iii. When seizing a computer, extreme care should be exercised in performing any keyboard strokes or mouse clicks as this may alter the evidence, or destroy the finger prints. All actions must be recorded.

iv. Only trained and qualified personnel should conduct seizure process.

Before you begin

I. Ensure you have the appropriate power and authority to search and seize.

II. Formulate a plan and course of action that you would undertake. Gathere as much information as possible about the place where search and seizure is to be conducted. After the suspect computer(s) is(are) shortlisted by the investigation officer, he should collect as much details as possible about the suspect computer(s) by quickest[1] possible means and if need be in consultation with an expert before embarking on search and seizure of electronic evidence.

III. This information should be on following issues:

   i. Location of Suspect Computer(s)

   ii. No. of Computers that might be involved in the crime

[1] Due to ephemeral nature of electronic evidence as well possibility of its deliberate destruction by the suspect.

iii. Total numbers of computers at site.

iv. Whether suspect computer(s) is(are) part of LAN, WAN, intranet and whether connected with Internet or is it a stand alone isolated Personal Computer?

v. Is there a system administrator?

vi. Whether suspect is the custodian of the suspect computer or a third party is the custodian?[2]

vii. Whether the system is password protected?

viii. Operating system involved

ix. Hard Disk capacities of the suspect system(s)[3]

x. Computer skill-level of suspect[4]

xi. Best time for access to computer[5]

xii. Requirement of a search warrant, if any

xiii. Criticality of time factor

IV. Determine the role of the computer, in the crime you are investing. This will help you determine what to look for.

V. Answering the following questions will help determining the role of the computer in the crime:

i. Is the computer contraband of fruits of a crime? For example, was the computer software or hardware stolen?

ii. Is the computer system a tool of the offense? For example, was the system actively used by the suspect to commit the offense? Were fake

[2] In case of third party custody, chances of booby traps will be less.

[3] This will decide the capacities of the hard disks required to image the suspect hard disk.

[4] To evaluate whether the computer could be booby-trapped or not?

[5] It is best to access the system in the presence of the suspect so that allegations of mishandling and tampering can be negated and passwords etc. ascertained, if necessary.

Identities or other counterfeit documents prepared using the computer, scanner, and color printer?

   iii. Is the computer system only incidental to the offense, i.e., being used to store evidence of the offense? For example, is a tax evader maintaining his manipulated records in his computer?

   iv. Is the computer system both instrumental to the offense and a storage device for evidence? For example did the suspect sent the ransom note through e-mail using his computer.

VI. Once the computer's role is understood, the following essential questions should be answered:

   i. Do you intend to seize hardware and are you equipped for that?

   ii. Do you intend to seize software and are you equipped for that?

   iii. Do you intend to seize data and you equipped for that?

   iv. Will you only seize, or you would have to acquire the evidence also at site? Such a situation may arise if it is not possible to physically shift the suspect machine.

VII. If acquisition of evidence is to be done at the site, summon a computer forensic officer. Such an eventuality may arise during the course of seizure. In such instances the best option is not to proceed any further, summons an computer forensic officer and secure the place till his arrival.

At Scene of Search and Seizure

I. Follow the pre-search procedure as laid down for physical searches. If possible, have yourself and the equipments you are carrying searched in the presence of witnesses. Ensure you have the appropriate authority to search and seize. Requisition the requisite numbers of witnesses.

II. Immediately request all present to leave and ensure all activities on computers both the suspect computer (if known) as well as other[6] computers in the vicinity are stopped.

III. Photograph the network connections and modem connections to the suspect computer (if known) and disconnect the modem from the power supply and network connection from the computer.[7]

IV. Minutely inspect the scene of crime for clues such as:

   i. Computer Printouts in room, on table, in drawers, in dustbins etc.

   ii. Passwords: On casing of computers, on tabletops, stickers, walls etc.

   iii. Manuals and reference books pertaining to computers

   iv. Physical Evidence such as documents, visiting cards, scribbling pads etc. On examination, relevant physical evidence should be inventoried for seizure.

V. Preliminary examination of witnesses (including system administrator) and suspects (if present) to elicit further information regarding the hardware, software and topography of the computers and any other clues regarding physical evidence.

VI. Minute survey of the scene of search to locate the suspect computer and its visual examination to ascertain whether there are any unusual connections, in which case, the help of expert must be sought if already not sought. Seized reference manuals & System Administrator MAY ALSO BE OF HELP.

VII. Photograph the scene of location of the suspect computer as well as the suspect computer itself from all angles showing in particular:

   i. All network connections

[6] Since other computers can be used to tamper the data in the suspect computer.

[7] So that data in the suspect computer is isolated from the network and possibility of its tampering can be eliminated.

ii. Modem Connections

iii. Power supply connection

iv. Peripheral Connections

v. The screen, if the computer is on.

VIII. Label all connections to the computer (network, modem and between CPU and peripherals), giving a separate set of numbers to each socket and corresponding connector by affixing identical stickers on corresponding set of socket and connector.

IX. Note down the particulars of the information on the screen (if the computer is on). Make a sketch of the scene of suspect computer showing all details particularly:

i. Location of the physical evidence short-listed for seizure

ii. Various connections to the computer and of computer peripherals, depicting the label nos.

iii. Various drives connected to the computer i.e. CD ROM, Floppy Drives, Zip Drive etc.

X. Disconnect the power supply to the printer connected to the suspect computer.

XI. If the computer is on

i. Ensure that all drives are empty (such as CD ROM, Floppy Drives etc)

ii. Locate the socket from where the suspect computer is powered and pull off the cord[8] from that socket.[9] In case of Laptops, in addition to disconnection of power supply, the batteries should also be removed.

[8] This may result in loss of information in RAM of suspect computer and occasional crashing of computer, which will be rare in case of stand-alone computers. However, the usual shutting down of computer may result in a booby trap where the suspect computer may be reformatted altogether.

[9] This is done because if power supply id pulled off from the main power socket, the computer can still remain on in case it is powered through a UPS.

XII. Photograph the suspect computer with power supply disconnected.

XIII. In case the computer is off, disconnect the power supply to the computer CPU for safety reasons.

At this stage, please ensure that irrespective of the condition in which you got the suspect computer the computer in question now should be .

i. In an off condition, with power cord disconnected

ii. All removable drives are empty

iii. The Suspect computer is in a stand-alone condition.

XIV. Remove the casing of the computer.

XV. Document and Photograph the internal configuration of the computer.

XVI. Disconnect the power supply from the all the hard drives connected after labeling the cords and photograph the same.

If you are using some other bootable and seizure software

I. Find out the keys to press, to enter the setup and change the booting sequence. (The keys for entering the setup of popular computers are annexed.) This is essential since for seizing the suspect computer, it should boot from your trusted operating system, stored on the storage media with you.

II. Connect the power cable to the computer and switch it on. Press the required keys immediately to enter the setup. Change the booting sequence so that the computer boots from the drive compatible with the storage media on which your booting and seizure software would be inserted: A: if it is on a floppy or Cd-Rom if it is on the CD-Rom. Save the changes made.

III. Shut down the computer

IV. Insert the bootable and seizure software in the appropriate drive.

V. Re-boot the system, and complete the process of seizure as outlined in the working manual of that software

If you are using Cyberckeck bootable software containing Trueback

The Trueback bootable software supplied with Cybercheck provides you the functionality of changing the booting sequence after booting the computer with Trueback and thereafter running the Bootwiz.

It also helps you in preparing the physical seizure memo (on paper, which is a requisite till such times The Evidence Act is amended), and also prepares a digital seizure memo, which it then transfers on a floppy for record. During the completion of the process of seizure or seizure and acquisition it asks you to type in information regarding the case under investigation which should be typed in with accuracy and care.

I. Insert the Trueback software in the appropriate drive. If it is on a floppy in the A: drive. If Trueback is on a CD-Rom, it should be inserted in the CD-Rom as soon as the computer is switched on following the procedure as enumerated in the following steps.

II. The system will boot from Trueback software, irrespective of the booting sequence, since all the drives are disconnected, except the one containing the Trueback.

    i. In case the software was on a CD-Rom and was inserted after switching on the computer, the system will show disk error. Press any key after inserting the CD-Rom. The system should boot from the CD-Rom.

III. On A: prompt, run Bootwiz and change the booting sequence in the following order, if already not in this order:

IV. First the drive in which Trueback software exists, i.e. CDROM or Floppy.

V. Then the other removable media other than that specified in (a) above.

VI. Lastly the HDD i.e. C: drive.

VII. Ensure that this booting sequence is saved in the CMOS and on display of the changed sequence, exit and shut down the system.

VIII. Reconnect the power supply to the Hard disks[10].

IX. If the option of "seize and acquisition" is to be exercised connect as a slave a hard disk of a larger capacity than the one to be seized to the suspect computer. Ensure that it is formatted and sterile, and its serial number has been recorded by you. While exercising this option, you should be adequately trained or should seek assistance from an authorized person who is adequately trained on working with Trueback.

X. Switch on the computer.

XI. On A: run Trueback. For assistance refer to the working manual.

XII. Choose one of the options, i.) Seize or ii) Seize and Acquire and follow the instructions. Please refer to the working manual in case of doubt.

XIII. Provide the requisite information as and asked for by the software

XIV. Note down the information as displayed by the software and prompted to be recorded by you.

XV. Follow the instructions and click on the "next" button only when satisfied that the instructions have been complied with or are in accordance with what you intended to type in.

XVI. At the end of the process you would have

[10] So that HDD is brought into play now so that it can be acquired. However it has been ensured that the suspect system boots from Trueback only.

a. Completed the physical seizure memo with all the requisite details, which you must get it signed by the witnesses, suspect and sign it yourself

b. The software would have prepared the digital seizure memo contained in the four floppies called the Cybercheck Seizure floppy (CSF). One of them is to be retained by you, the second one is for the suspect, the third one is to be sent to the concerning court, and the last one to the forensic laboratory for the analysis of the seized evidence.

c. In case you had opted for the Seize and Acquire option a bit-stream copy of the evidence that has been seized would be on the sterile media connected by you as slave (*step XXVII) in the ***.PO1 format.

XVII. On completion shut down the system and follow the guidelines for handling, packing and transportation digital evidence.

Acquisition of Evidence

This is the crucial stage were a bit-stream backup of the seized evidence is prepared. This bit-stream backup is then to be used for analysis. Thus it is essential that this process be completed under due supervision and the copied image of the seized evidence should result in the same message digest.

The seized computer or storage media shall be sent to a computer forensic laboratory. The investigating officer should furnish details of the software used by him for seizing the evidence. If he has used Cybercheck's bootable software Trueback, he should forward the Cybercheck seizure floppy (CSF), which was prepared during the course of seizure also. The process of acquisition should be completed in the laboratory by a qualified personal, using a software which is compatible with the software used for seizing.

Trueback fulfills both the requirements of seizure and acquisition.

I. Attach an appropriate storage device to the Computer Forensic work Station. It should be ensures that it is of a larger capacity that the storage media that is to be bit-streamed. It should be sterile and formatted.

II. Boot the workstation in a trusted environment and run the appropriate acquisition software. (Trueback in case Cybercheck is being used)

III. Choose the appropriate configuration: disc to disc or through parallel port as the case maybe.

   i. Provide the requisite information as and asked for by the software

   ii. Note down the information as displayed by the software and prompted to be recorded by you.

   iii. Follow the instructions and click on the "next" button only when satisfied that the instructions have been complied with or are in accordance with what you intended to type in.

IV. Start the acquisition process

V. At completion, you should have

   i. A bit stream backup of the seized evidence on the desired sterile media.

   ii. The software should authenticate the bit-stream backup with the original evidence, by Hashing them..

VI. The acquired image if it is successfully authenticated, should be used for analysis purposes, else the whole process should be repeated till such times an authenticated backup is got.

Analysis.

This is the most cumbersome and tedious part. Due caution should be exercised to authenticate bit-stream image each time it is used for analysis. Necessary logs should be maintained for each action taken. Available softwares have different capabilities. The problem is further aggravated because of the huge amount of information that can now be stored in various storage medias. It would be a Herculean task for a computer forensic analyst to come up with relevant evidence if the investigating officer is not in a position to tell him what he is looking for, or what information may be of help in the investigation of the said case.

The huge amount of information available raises the issue of privacy of the concerning person from whom the evidence has been seized. Utmost care and restrain has to be exercised by the Analyst and the Investigating officer, while handling such evidence.

Note: Pease refer "Manual or investigation of Computer related Crimes" by Ashok Dohare for further details.

Setting up of the Computer Forensic Laboratory

Backdrop

The Department of Information Technology, Ministry of Communications and Information Technology, Government of India allotted a one-year Research Project 'Identification of appropriate technologies and procedures for handling and analyzing digital evidence" in May 2001 The total outlay of the project was Rs. 50 lakhs, which included Rs. 34 lakhs for equipment. The equipment was to mainly consist of hardware and software for handling and analyzing data that would be used to analyze the features of the existing hardware and software products in the international market in the field of cyber forensics, the results of which will be used to indigenously design the software by C-DAC (Formerly Electronic Research and Development Center of India - ERDCI), Government of India, Thiruvanthapuram. The equipment was also intended to be used for imparting training to officers undergoing basic course and cyber crime course training at the Academy in the long run. This availability of finance, mandate and the excellent existing infrastructure at the academy resulted in the establishment of the lab at the Academy.

The Cyber Forensic Lab at the Academy consists of state-of-art, especially constructed 17 workstations, which are equipped with the internationally accepted best software in the field of cyber forensics in the world.

16 of the workstations consist of standard PCs, which have been suitably modified as per the needs of a Cyber crime investigator or a Cyber Forensic Expert. All the workstations have hot swappable HDDs so that the suspect hard drive and target hard drive can be connected to the workstation without opening of the workstation CPU. Similarly, workstations also have multiple 3.5" Floppy Diskette

Drives, multiple CD ROM read and write drives also. The 13th workstation is the world-renowned DIBS system, which is an integrated hardware and Software cyber forensic solution.

The Laboratory was inaugurated by Sh Rajeeva Ratna Shah Secretary Department of Information Technology MCIT Delhi.

The lab has the most widely internationally accepted cyber forensic software that is commercially available. Besides the commercially available softwares, the research team has consciously downloaded some of the best freeware cyber forensic softwares for experimentation and distribution to trainees to arouse their interest in the area of cyber forensics. The lab has also tried successfully to get non-commercial, proprietary softwares such as ilook (developed by a UK Law Enforcement Officer), using the vast goodwill that the Academy enjoys all over the world. Efforts are underway to equip the lab with hardware/software solutions for forensically extracting data from Cellular phones and Personal Digital Assistants which should materialize by March, 2003. The list of available software in the lab is as follows:

Commercial Softwares

i. EnCase
ii. FastBloc (with EnCase)
iii. NTI Tools
iv. Expert Witness
v. Stellar

vi. DIBS along with Portable Evidence Recovery Unit, Rapid Action Imaging Device, Portable Evidence Analyzer Etc (an integrated hardware and Software forensic solution)

Non-Commercial Proprietary

Softwares

ILook

Freeware Softwares

i. Directory Snoop

ii. PC Inspector

iii. DRS

The lab is under a constant upgradation. Because of sophisticated nature of softwares and hardware, although presently the laboratory is been used principally for research purpose except giving demonstration to trainees, not too distant in future, the lab will be utilized for training of IPS officers in the important area of cyber crimes and cyber forensics, besides the research in this area.

Laws Relating to Computer Crimes in Various Nations

AUSTRALIA

Federal legislation:

THE CYBERCRIME ACT 2001

The Cybercrime Act 2001 amended the Criminal Code Act 1995 to replace existing outdated computer offences.

478.1 Unauthorised access to, or modification of, restricted data

(1) A person is guilty of an offence if:

(a) the person causes any unauthorised 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 unauthorised; 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 1, 2000:
Section 10:

§ 52. Administrative Penalty Clause

(1) 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
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 judgement 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 in November 2000 adopted new articles in the Criminal Code on computer crime, in effect from February 13, 2001. The four main problems of computer forgery, computer fraud, hacking and sabotage are made criminal offences.

IV. COMPUTER HACKING

Article 550(b) of the Criminal Code:

§1. Any person who, aware that he is not authorised, 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 in §1 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 in §§ 1 and 2 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 in §§ 1 and 2 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 commercialises data which is stored, processed or transmitted by a computer system and by means of which the offences specified in §§1-4 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 in §§ 1-5 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 in §§1-3, 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 14 JULY 2000

Art. 1

The following provisions are added to the Special Part of Decree-Law No. 2,848 of 7 December 1940 - Penal Code:

Improper social security appropriation

Art. 168-A. Failure to pass on to social security the contributions withheld from taxpayers, within the time period and in a legal or conventional fashion:

Penalty - imprisonment for 2 (two) to 5 (five) years, and fine.

1 Subject to the same penalty is anyone who fails to:

- I withhold, within the legal time period, any contribution or other amount intended for social security that has been deducted from any payment made to the insured or to third parties, or collected from the public:
- II withhold contributions owed to social security that have included accountable expenses or costs relating to the sale of products or the provision of services:
- III pay the benefit owed to the insured when the respective portions or amounts have already been reimbursed to the company by social security.

2 The punishment does not apply if the agent spontaneously states, confesses and makes payment of the contributions, amounts or values, and provides appropriate information to social security, in the manner defined in the law or in regulations, prior to the initiation of the legal action.

3 The judge is empowered to waive the application of the penalty, or apply only that of the fine, if the agent is primary, and with a good behavioral background, so long as:

- I he has, following the initiation of the legal action and before the accusation is made, seen to the payment of the social security contributions, including accessory amounts; or
- II the value of the contributions owed, including accessory amounts, is less than or equal to that established by social security, administratively, as being the minimum for the adjudication of its fiscal executions.

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 computer system or the data bank of the public administration for purposes of achieving an improper advantage for himself or for some other person, or of causing damages.

Penalty imprisonment for 2 (two) to 12 (twelve) years, and fine.

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 (three) months to 2 (two) years, and fine.

Special paragraph. The penalties are increased by one-third to one-half if damage to the public administration or to the administered individual results from the modification or alteration.

Misappropriation of social security contributions

Art. 337-A.

Exceeding or reducing social security contributions and any accessory amounts through the following types of conduct:

I omission, from the payroll records or from the information document required by social security legislation, of any insured employee, entrepreneur, freelance employee or independent worker, or those who provide services:

II failure to enter on a monthly basis into the accounting records of the company the amounts deducted from the insured employees, or those owed by the employer or by receiver of services;

III the omission, total or partial, of income or profits earned, remuneration paid or credited, and other factors which generate social security contributions:

Penalty imprisonment for 2 (two) to 5 (five) years, and fine.

1 The punishment does not apply if the agent spontaneously states and confesses the contributions, amounts or values, and provides appropriate information to social security, in the manner defined in the law or in regulations, prior to the initiation of the legal action.

2 The judge is empowered to waive the application of the penalty, or apply only that of the fine, if the agent is primary, and with a good behavioral background, so long as:

I (VETOED)

II the value of the contributions owed, including accessory amounts, is less than or equal to that established by social security, administratively, as being the minimum for the adjudication of its fiscal executions.

3 If the employee is not an individual, and his monthly payroll does not exceed R$ 1,510.00 (One thousand, five hundred and ten reals), the judge may reduce the penalty by one-third to one-half, or apply only the fine.

4 The value referred to in the above paragraph will be adjusted on the same dates and using the same indices as the adjustments to social security.

Art. 2

Articles 153, 296, 297, 325 and 327 of Decree-Law No. 2,848 of 1940 take effect with the following alterations:

Art. 153. ....

1 A To divulge, without due cause, secret or reserved information, as defined under the law, whether contained or not in the information systems or the data bank of the public administration:

Penalty imprisonment for 1 (one) to 4 (four) years, and fine.

1 (original special paragraph) ....

2 When damage to the public administration results, the penal action will be unconditional.

Art. 296.

1 III - whoever alters, falsifies or makes improper use of trade marks, logos, initials or any other symbols utilized by or identifying sections or entities of the public administration.

Art. 297

3 Subject to the same penalties will be anyone who enters or causes to be entered:

I into the payroll records or any information document to be used as evidence before the social security administration, any person who is not categorized as being insured by law;

II into the work record or the social security records of the employee, or into any document which is presented as proof to social security, a false statement or one that diverges from what should be stated.

4 Subject to the same penalties will be anyone who omits from the documents mentioned in 3 the name of the insured and his personal data, his remuneration, the validity period for the labor contract or the provision of services.

Art. 325.

1 Subject to the same penalties is anyone who:

I permits or facilitates through attribution, the supply and loan of the password or [in] any other way, access by unauthorized persons to the information systems or data bank of the public administration;

II improperly makes use of restricted access.

2 If damage is caused to the public administration or to anyone else, based on the action or omission:

Penalty imprisonment for 2 (two) to 6 (six) years, and fine.

Art. 327

1 A public employee who performs a position, job or function in a para-state organization is comparable to one who works for a company that provides services on a contract or agreement basis for the execution of any typical activity of the public administration.

CANADA

Data Modification, Network Interference, Network Sabotage, and Virus Dissemination

PART XI: **Wilful And Forbidden Acts In Respect Of Certain Property**

430. (1) Every one commits mischief who wilfully
(a) destroys or damages property;
(b) renders property dangerous, useless, inoperative or ineffective;
(c) obstructs, interrupts or interferes with the lawful use, enjoyment or operation of property; or
(d) obstructs, interrupts or interferes with any person in the lawful use, enjoyment or operation of property.

(1.1) Every one commits mischief who wilfully
(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of data; or
(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

(2) Every one who commits mischief that causes actual danger to life is guilty of an indictable offence and liable to imprisonment for life.

(3) Every one who commits mischief in relation to property that is a testamentary instrument or the value of which exceeds five thousand dollars
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
(b) is guilty of an offence punishable on summary conviction.

(4) Every one who commits mischief in relation to property, other than property described in subsection (3),
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or
(b) is guilty of an offence punishable on summary conviction.

(5) Every one who commits mischief in relation to data
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years; or
(b) is guilty of an offence punishable on summary conviction.

(5.1) Every one who wilfully does an act or willfully omits to do an act that it is his duty to do, if that act or omission is likely to constitute mischief causing actual danger to life, or to constitute mischief in relation to property or data,
(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years; or
(b) is guilty of an offence punishable on summary conviction.

(6) No person commits mischief within the meaning of this section by reason only that
(a) he stops work as a result of the failure of his employer and himself to agree on any matter relating to his employment;
(b) he stops work as a result of the failure of his employer and a bargaining agent acting on his behalf to agree on any matter relating to his employment; or

(c) he stops work as a result of his taking part in a combination of workmen or employees for their own reasonable protection as workmen or employees.

(7) No person commits mischief within the meaning of this section by reason only that he attends at or near or approaches a dwelling-house or place for the purpose only of obtaining or communicating information.

(8) In this section, data has the same meaning as in section 342.1.

Data Interception, Unauthorized Access, Additional Virus Dissemination

PART IX: Offences Against Rights Of Property

342.1

(1) Every one who, fraudulently and without colour 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.

Possession of device to obtain computer service

342.2

(1) Every person who, without lawful justification or excuse, makes, possesses, sells, offers for sale or distributes any instrument or device or any component thereof, the design of which renders it primarily useful for committing an offence under section 342.1, under circumstances that give rise to a reasonable inference that the instrument, device or component has been used or is or was intended to be used to commit an offence contrary to that section,

(a) is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years; or

(b) is guilty of an offence punishable on summary conviction.

Additional Data Interception Provisions
PART VI: **Invasion Of Privacy**

184.

(1) Every one who, by means of any electro-magnetic, acoustic, mechanical or other device, wilfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

(2) Subsection (1) does not apply to

(a) a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;

(b) a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;

(c) a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

(i) if the interception is necessary for the purpose of providing the service,

(ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or

(iii) if the interception is necessary to protect the person's rights or property directly related to providing the service; or

(d) an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission.

Data Theft

PART IX: **Offences Against Rights Of Property**

322. (1) Every one commits theft who fraudulently and without colour of right takes, or fraudulently and without colour of right converts to his use or to the use of another person, anything, whether animate or inanimate, with intent

(a) to deprive, temporarily or absolutely, the owner of it, or a person who has a special property or interest in it, of the thing or of his property or interest in it;

(b) to pledge it or deposit it as security;

(c) to part with it under a condition with respect to its return that the person who parts with it may be unable to perform; or

(d) to deal with it in such a manner that it cannot be restored in the condition in which it was at the time it was taken or converted.

(2) A person commits theft when, with intent to steal anything, he moves it or causes it to move or to be moved, or begins to cause it to become movable.

(3) A taking or conversion of anything may be fraudulent notwithstanding that it is effected without secrecy or attempt at concealment.

(4) For the purposes of this Act, the question whether anything that is converted is taken for the purpose of conversion, or whether it is, at the time it is converted, in the lawful possession of the person who converts it is not material.

Computer Related-Fraud

PART X: **Fraudulent Transactions Relating To Contracts And Trade**

380. (1) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service,

(a) is guilty of an indictable offence and liable to a term of imprisonment not exceeding ten years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter of the offence exceeds five thousand dollars; or

(b) is guilty

(i) of an indictable offence and is liable to imprisonment for a term not exceeding two years,

or

(ii) of an offence punishable on summary conviction, where the value of the subject-matter of the offence does not exceed five thousand dollars.

(2) Every one who, by deceit, falsehood or other fraudulent means, whether or not it is a false pretence within the meaning of this Act, with intent to defraud, affects the public market price of stocks, shares, merchandise or anything that is offered for sale to the public is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years.

381. Every one who makes use of the mails for the purpose of transmitting or delivering letters or circulars concerning schemes devised or intended to deceive or defraud the public, or for the purpose of obtaining money under false pretences, is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years

CHILE

Law Relative to Information/Computer Crimes

Article 1 The one that maliciously destroys or makes unusable a system of information processing or its parts or components, or prevents or modifies its operation, will be undergo the punishment of prison from average to maximum degree. If, as a result of this action, the data contained in the system will be affected, the punishment indicated in the previous interjection will be applied in its maximum degree.

Article 2 The one that attempts illegally to seize, to use, or to know the information contained in an information processing system or to intercept or interfere or have access to it, will be punished with a minor to medium jail sentence.

Article 3 The one that maliciously alters, damages or destroys the data contained in a system of information processing, will be punished with a prison sentence of minor to a medium degree.

Article 4. The one that maliciously reveals or spreads the data contained in an IS will undergo the punishment with a prison sentence of minor to medium sentence. If the person who incurs these conducts Is the person in charge of the IS, the punishment will be increased in degree

PEOPLES REPUBLIC OF CHINA

Regulation on Protecting the Safety of Computer information (Order no 147)
Computer Information network and Internet Protection and Management Regulations (1997)

Decree No. 147 of the State Council of the Peoples Republic of China, February 18, 1994. Regulations of The Peoples Republic of China on Protecting the Safety of Computer Information System: Chapter 4 - Legal Responsibilities.

Article 23 - The public security organisations shall give warnings or may impose maximum fines of 5.000 Yuan on individuals and 15.000 Yuan on organisations in cases when they deliberately input a computer virus or other harmful data endangering a computer information system, or in a case when they sell special safety protection products for computer information systems without permission. Their illegal income will be confiscated and a fine shall be imposed in the amount of one to three times as much as the illegal income (if any).

1994 Regulations 1994

Warnings may be given, fines imposed and illegal income confiscated in cases of deliberate input of computer virus or selling special safety protection products without permission.

1997 Regulations

Prohibition of use of Internet to:

A. harm national security, disclose state secrets, conduct illegal activity etc. (Art. 4), punishable by relevant State regulations (Art. 19);

B. transmit information inciting illegality or overthrow of the Government etc. (Art. 5), punishable by warnings, confiscation of illegal income, and fines of not more than 5,000 RMB for individuals or 15,000 RMB for Internet service providing units (Art. 20).

Prohibition of activities harming the security of computer information networks including:

A. unapproved use of computer networks or resources, change of network functions, adding/ deleting/altering stored data etc.;

B. creation or transmission of computer viruses, punishable as for Art. 5.

HONGKONG

Telecommunication Ordinance: Section 27A: Unauthorized access to computer by telecommunication:

(1) Any person who, by telecommunication, knowingly causes a computer to perform any function to obtain unauthorized access to any program or data held in a computer commits an offence and is liable on conviction to a fine of $ 20000.

(2) For the purposes of subsection (1)-

I. the intent of the person need not be directed at-
   i. any particular program or data;
   ii. a program or data of a particular kind; or
   iii. a program or data held in a particular computer;

II. access of any kind by a person to any program or data held in a computer is unauthorized if he is not entitled to control access of the kind in question to the program or data held in the computer and-
   i. he has not been authorized to obtain access of the kind in question to the program or data held in the computer by any person who is entitled;
   ii. he does not believe that he has been so authorized; and
   iii. he does not believe that he would have been so authorized if he had applied for the appropriate authority.

(3) Subsection (1) has effect without prejudice to any law relating to powers of inspection, search or seizure.

(4) Notwithstanding section 26 of the Magistrates Ordinance (Cap 227), proceedings for an offence under this section may be brought at any time within 3 years of the commission of the offence or within 6 months of the discovery of the offence by the prosecuter, whichever period expires first.

Section 161: Access to computer with criminal or dishonest intent.

(1) Any person who obtains access to a computer-
   a. with intent to commit an offence;
   b. with a dishonest intent to deceive;
   c. with a view to dishonest gain for himself or another; or
   d. (d) with a dishonest intent to cause loss to another,

   whether on the same occasion as he obtains such access or on any future occasion, commits an offence and is liable on conviction upon indictment to imprisonment for 5 years.

(2) For the purposes of subsection (1) "gain" and "loss" are to be construed as extending not only to gain or loss in money or other property, but as extending to any such gain or loss whether temporary or permanent; and-

   (a) "gain" includes a gain by keeping what one has, as well as gain by getting what one has not; and

   (b) "loss" includes a loss by not getting what one might get, as well as a loss by parting with what one has.

CZECH REPUBLIC

2.1.1. Legislation on the protection of intellectual property rights
b) Crime in information technology

Hacking in IT and programmes

§ 152 of the Criminal Code -	Infringement of copyright
§ 182 of the Criminal Code -	Impairing and endangering the operation of public utility facilities
§ 249 of the Criminal Code -	Unauthorised use of other people's articles
§ 257a of the Criminal Code -	Damaging and misusing records in information stores

Unlawful conduct in the electronics trade

§ 121 of the Criminal Code -	Harming the consumer
§ 127 of the Criminal Code -	Breaching the binding regulations of economic relations
§ 128 of the Criminal Code -	Misuse of information in business relations
§ 250 of the Criminal Code -	Fraud

ESTONIAN

Chapter 14
Computer and work place related crimes

Paragraph 268. Computer Fraud

This pertains to property other than your own when used for profit advantage, exchange of information, and any changing of software that results in a disadvantage to the owner. This includes such things as computer programs, removing, adding or blocking data. These offenses are punishable by fines or bodily arrest and can result in incarceration for one to six years.

Paragraph 269. The destruction of programs and data in the computer.

(1) For the wrongful use, destruction, damaging, or blocking of data or programs in the computer, the penalty is the levying of a fine or personal arrest.

(2) Same as above except for the following the penalty is bodily arrest and a prison sentence of up to 2 years

- (a) when it has caused a large loss of assets
- (b) when directed against the main government files or auxiliary government information files
- (c) when pre-planned by a group of people

Paragraph 270. Computer Sabotage

(1) Information or program inserting, exchanging, blocking, for the purpose of restricting computer operations or telecommunication systems is punishable by fine, arrest or up to two years imprisonment

(2) Same as above when:

- (a) when it has caused material loss or
- (b) when directed to restrict government operations--the punishment is up to 4 years imprisonment.

Paragraph 271. Unauthorized use of computer, computer system, and network.

(1) Person or persons removing pass-words, personal and protection codes of the computer, computer system or computer network are subject to a fine or arrest.

(2) Same as above:

- (a) if it is a repeated offense or
- (b) when it has caused material loss
- (c) when government secrets are used, or computers, computer systems, or computer networks with designated government information contained therein, the penalty is a fine, arrest or up two years in prison.

Paragraph 272. Damaging or blocking the computer network connections

The offense of damaging or blocking computer network connections by technical means carries a penalty of a fine, or arrest or imprisonment up to 2 years.

Paragraph 273. Knowingly spreading a computer virus

(1) The penalty for this is a fine
(2) same as above
  (a) repeated action or
  (b) when it has caused material loss or
  (c) if the virus was spread to government computer systems or
  (d) or if the virus was spread to the world wide network, the penalty is a fine, or an arrest or up to 4 years imprisonment.

Paragraph 274. Distributing passwords

(1) Distributing passwords of computers or computer systems, or computer networks is subject to a fine or an arrest.
(2) Same as above when giving out passwords that reveal personal information, government secrets, or information designed for designated purposes. Penalty for these offenses is arrest or up to 2 years imprisonment.
(3) Same as above
  (a) when the purpose is monetary gain or
  (b) when it has caused material loss The penalty is arrest or imprisonment up to 4 years.

Paragraph 275 Providing false information to the business world

(1) For knowingly providing false or incorrect information, the penalty is a fine
(2) Same as above
  (a) when the purpose is monetary gain or
  (b) for repeat offenses or
  (c) for seeking and obtaining illegal profit or gains or
  (d) to cause a material loss. The penalty is a fine, or arrest or imprisonment up to 1 year

Paragraph 276 Fraudulently obtaining information from state or local government

The unlawful removal of information from state or local governments when

(1) seeking and obtaining illegal profit and gain or to apply and receive profit
(2) ruining personal, family and private lives. The penalty is a fine, or arrest, or imprisonment up to 2 years

FINLAND

Penal Code Chapter 38 Section 8:
Data trespass.

Any person who, by using an identification code that does not belong to him or by breaking through a corresponding protective system unjustifiable, breaks into a computer system where data are processed, stored or transmitted by electronical or other technical methods or into a separately protected part of such a system, shall be sentenced for data trespass to fines or imprisonment not exceeding one year.

For data trespass is also sentenced any person without breaking into a computer system or a part thereof, uses a special technical device to unjustifiably obtain information that is stored in such a computer system.

Attempt is also punishable.

This Section will only be applied if the act is not punishable as a more severe offense.

FRANCE

The new Penal Code, in effect since March 1, 1993
Chapter III: ATTACKS ON SYSTEMS FOR AUTOMATED DATA PROCESSING

Article 323-1:

The act of fraudulently gaining access to, or maintaining, in all or part of an automated data processing system is punishable by imprisonment not exceeding one year and a fine of up to 100.000 F.

Whenever this results in the suppression or modification of data contained in the system, or an alteration in the functioning of the system, the act is punished by imprisonment not exceeding two years and a fine up to 200.000 FF.

Article 323-2:

The act of hindering or of distorting the functioning of an automated data processing system is punishable by imprisonment not exceeding three years and a fine up to 300.000 FF.

Article 323-3:

The act of fraudulently introducing data into an automated data processing system or of fraudulently suppressing or modifying data contained therein is punishable by imprisonment not exceeding three years and a fine up to 300.000 FF.

Article 323-4:

Participation in a formed group or in an agreement with preparation in mind, characterized by one or more material acts, of one or more offenses provided for by Articles 323-1 to 323-3, is punishable by the sentences provided for the most serious offense committed.

GERMANY

Criminal Law

Sec. 202a - Data spying

(1) Anybody who without authority procures himself or another data which are not meant for him and which are specially secured against unauthorised access shall be sentenced to imprisonment not exceeding 3 years or to a fine.

(2) Data within the meaning of Subsection (1) shall be deemed to be only those which are stored or transmitted electronically, magnetically, or in any other not directly perceptible way.

Sec. 203 - Violation of private secrets

(1) Anybody who without authority discloses another's secret, especially one relating to the personal sphere of life or an industrial or business secret that has been entrusted to him or has otherwise become known to him in his capacity as

1. physician, dentist, veterinarian, dispensing chemist or member of another healing profession requiring state regulated training for the exercise of the profession or for the bearing of the professional title,
2. professional psychologist with a state recognised scientific final examination,
3. lawyer, patent agent, notary public, defence counsel in proceedings regulated by law, certified public accountant, sworn auditor, tax adviser, authorised tax agent, or an organ, or member of an organ, of a society of certified public accountants, auditors, or tax advisers,
4. marriage, family, educational, or youth counsellor as well as addiction counsellor at a counselling agency that is recognised by public authority or by a corporation, institution, or foundation of public law,

   4a. member or agent of a recognised counselling agency under Sec. 218b (2) (No. 1),
5. state recognised social worker or state recognised social educationalist or
6. member of an enterprise of private health, accident, or life, insurance or of an accounting office for private physicians,

shall be sentenced to imprisonment not exceeding one year or to a fine.

(2) Likewise shall be punished anybody who without authority discloses another's s

1. holder of a public office,
2. a person with special obligations with regard to the civil service,
3. a person carrying out tasks or responsibilities under the Personnel Representation Law,
4. member of an investigation committee acting for a Federal, or State, legislative body or of any other committee or council who is not himself a member of the legislative body, or as an assistant of such committee or council, or
5. an officially appointed expert who has been formally obligated for the conscientious compliance with his duties on the basis of legal provisions Equivalent to a secret within the meaning of Sentence 1shall be individual information concerning personal or factual circumstances of another that have been recorded for purposes of public administration; Sentence 1 shall not

apply, however, where such individual information is disclosed to other public authorities or other agencies for purposes of public administration and this is not prohibited by law.

(3) Equivalent to the parties mentioned in Subsec. (1) shall be their professionally active assistants as well as persons who are working with them while learning the profession. In addition, after the person charged with the duty of protecting the secret has died, anyone who has obtained knowledge of the secret from the deceased or from gis estate shall be deemed equivalent to the parties mentioned in Subsec. (1) and those mentioned in Sentence 1.

(4) Subsections (1 - 3) shall also apply where the offender without authority disclose another's secret after the latter's death.

(5) If the offender discloses the secret for a consideration, or with the intention of enriching himself or another or to injure another, punishment shall be imprisonment not exceeding two years or a fine.

Sec. 204 - Exploitation of another's secret

(1) Anybody who without authority exploits another's secret especially an industrial or business secret which he is bound to keep confidential under Sec. 203, shall be sentenced to imprisonment not exceeding two years or to a fine.

(2) Sec. 203 (4) shall apply accordingly.

Sec. 263a - Computer fraud

(1) Anybody who, with a view to procuring himself of a third person any unlawful property advantage, causes prejudice to the property of another by influencing the result of a data proceeding activity through improper program design, through the use of incorrect or incomplete data, through the unauthorised use of data, or otherwise through any unauthorised interference with the transaction, shall be sentenced to imprisonment not exceeding five years or to a fine.

Sec. 269 - Forgery of probative data

(1) Anybody who, for the purpose of committing a deception in legal transactions, stores or alters probative data in such a way that a false or altered document would be present if the data were perceived, or makes use of data so stored or altered, shall be sentenced to imprisonment not exceeding five years or to a fine.

(2) The attempt shall be punished.

Sec. 270 - Deception in legal transactions in connection with data processing

Improperly interfering with a data processing activity in legal transactions shall be equivalent to deception in legal transactions.

Sec. 303a - Alteration of data

(1) Anybody who unlawfully deletes, suppresses, renders useless, or alters data (Sec. 202a (2)) shall be sentenced to imprisonment not exceeding 2 years or to a fine.

(2) The attempt shall be punished.

Sec. 303b - Computer sabotage

(1) Anybody who interferes with a data processing activity which is of vital importance to another enterprise, another business or a public authority by

1. committing an offence under Sec. 303a (1) or
2. destroying, damaging, rendering useless, removing or altering a data processing system or carrier

shall be sentenced to imprisonment not exceeding five years or to a fine.

(2) The attempt shall be punished

GREECE

Criminal Code Article 370C§2:

1. Every one who obtains access to data recorded in a computer or in the external memory of a computer or transmitted by telecommunication systems shall be punished by imprisonment for up to three months or by a pecuniary penalty not less than ten thousands drachmas, under condition that these acts have been committed without right, especially in violation of prohibitions or of security measures taken by the legal holder. If the act concerns the international relations or the security of the State, he shall be punished according to Art. 148.
2. If the offender is in the service of the legal holder of the data, the act of the preceding paragraph shall be punished only if it has been explicitly prohibited by internal regulations or by a written decision of the holder or of a competent employee of his.

HUNGARY

Penal Code Section 300 C:

Computer Fraud.

(1) Whoever, with the intent of obtaining for himself an unlawful gain, or by damaging, interferes with the results of electronic data processing, by altering programs, by erasing, by entering incorrect or incomplete data, or by other unlawful means commits an offence, imprisonment for a term not exceeding 3 years may be imposed.

(2) The punishment is

a) imprisonment not exceeding 5 years whenever the fraudulent offence causes conciderable damage.

b) imprisonment from 2 years until 8 years whenever the fraudulent offence causes exceptional conciderable damage.

(3) Whoever commits the offences under subsection (1)-(2) by using an electronic card for public or mobile telephone, or by altering the microprogram for the mobile telephone commits also fraud in connection with data.

IRELAND

Criminal Damage Act, 1991:
Section 5:

(1) A person who without lawful excuse operates a computer -

(a) within the State with intent to access any data kept either within or outside the State, or:

(b) outside the State with intent to access any data kept within the State, shall, whether or not he accesses any data, be guilty of an offense and shall be liable on summary conviction to a fine not exceeding £500 or imprisonment for a term not exceeding 3 months or both.

(2) Subsection (1) applies whether or not the person intended to access any particular data or any category of data or data kept by any particular person.

ICELAND

Penal Code § 228 Section 1:

The same penalty shall apply on any person who by unlawful manner obtains access to data or programs stored as data.

ISRAEL

The Computer Law of 1995, Section 4:

> Any person who, unlawfully obtains access to data in a computer, shall be sentenced to imprisonment not exceeding three years.
>
> With access to data means access to equipment's connected to computers or access activated through such equipment's, in addition to access defined as unlawful wiretapping according to the Law of 1979.

ITALY

Penal Code Article 615 ter:

Unauthorized access into a computer or telecommunication systems:

Anyone who enters unauthorized into a computer or telecommunication system protected by security measures, or remains in it against the expressed or implied will of the one who has the right to exclude him, shall be sentenced to imprisonment not exceeding three years.

The imprisonment is from one until five years:

1) if the crime is committed by a public official or by an officer of a public service, through abuse of power or through violation of the duties concerning the function or the service, or by a person who practices - even without a licence - the profession of a private investigator, or with abuse of the capacity of a system operator.
2) if to commit the crime the culprit uses violence upon things or people, or if he is manifestedly armed.
3) if the deed causes the destruction or the damage of the system or the partial or total interruption of its working, or rather the destruction or damage of the data, the information or the programs contained in it.

   Should the deeds of the 1st and 2nd paragraphs concern computer or telecommunication systems of military interest or (concerning) public order or public security or civil defence or whatsoever public interest, the penalty is - respectively- one to five years or three to eight years' imprisonment. In the case provided for in the 1st paragraph, the crime is liable to punishment only after an action by the plaintiff; the other cases are prosecutioned "ex-officio".

615 qua ter:

Illegal Possession and Diffusion of Access Codes to Computer or Telecommunication Systems:

Whoever, in order to obtain a profit for himself or for another or to cause damage to others, illegally gets hold of, reproduces, propagates, transmits or deliver codes, key-words or other means for the access to a computer or telecommunication system protected by safety measures, or however provides information or instructions fit to the above purpose, is punished with the imprisonment not exceeding one year and a fine not exceeding 10 million liras.

The penalty is imprisonment from one until two years and a fine from 10 until 20 million liras in the case of one of the circumstances numbered in 1 and 2 in the 4th paragraph of article 617-quater.

615 quinquies:

Diffusion of Programs Aimed to Damage or to Interrupt a Computer System:

Whoever propagates, transmits or delivers a computer program - edited by himself or by another - with the aim and the effect to damage a computer or telecommunication system, the data or the programs contained or pertinent to it, or rather the partial or total interuption or an alteration in its working, is punished with imprisonment not exceeding two years and fined not exceeding 20 million liras.

JAPAN

Unauthorized Computer Access Law (Law No. 128 of 1999)

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 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.

Prohibition of acts of facilitating unauthorized computer access

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.

Protective measures by access administrators

Article 5. The access administrator who has added an access control function to a specific computer shall endeavor to properly manage identification codes relating to that access control function and codes used to confirm such identification codes through that access control function, and shall always verify the effectiveness of that access control function, and, when he deems it necessary, shall endeavor to promptly take necessary measures to protect that specific computer from acts of unauthorized computer access, including the upgrading of the access control function concerned.

Assistance, etc., by Metropolitan and Prefectural Public Safety Commissions

Article 6.

1. The Metropolitan or Prefectural Public Safety Commission (each of the Area Public Safety Commissions in case of the Areas (that means the Areas mentioned in Article 51, paragraph 1, main part, of the Police Law (Law No. 162 of 1954); the same shall

apply hereafter in this paragraph) except the Area which comprises the place of the Hokkaido Prefectural Police Headquarters: the same shall apply hereafter in this Article), in case an act of unauthorized computer access is recognized to have been conducted and if, for the purpose of preventing a recurrence of similar acts, assistance is requested by the access administrator of the specific computer involved in that act of unauthorized computer access, attaching to such request any documents or articles regarding referential matters, such as the situations of operation and management of that specific computer at the time of that act of unauthorized access, shall provide, when it deems such request reasonable, that access administrator with assistance, including provision of relevant materials, advice and guidance, so that necessary emergency measures can be properly taken in accordance with the modus operandi of that act of unauthorized access or its cause to protect that specific computer from acts of unauthorized access.

2. The Metropolitan or Prefectural Public Safety Commission may entrust to a person to be stipulated by National Public Safety Commission Regulation with all or part of the work of implementing a case analysis (which means making a technical study and analysis on the modus operandi of the act of unauthorized computer access relating to that request and the cause of such act; the same shall apply in the following paragraph) which is necessary for the providing of the assistance mentioned in the preceding paragraph.
3. A person who has engaged in the work of implementing a case analysis entrusted by the Metropolitan or Prefectural Public Safety Commission in accordance with the preceding paragraph shall not reveal secret he or she has learned with regard to such implementation.
4. The necessary matters, other than those stipulated in the preceding three paragraphs, relating to the assistance mentioned in the first paragraph shall be stipulated by National Public Safety Commission Regulation.

Article 7.

1. The National Public Safety Commission, the Minister of International Trade and Industry and the Minister of Posts and Telecommunications shall publicize, at least once a year, the situation of occurrence of acts of unauthorized computer access as well as the situation of research and development of the access control function-related technology in order to help protect specific computers having access control functions from acts of unauthorized computer access.
2. In addition to the preceding paragraph, the State shall endeavor to assure the enlightenment and diffusion of knowledge regarding the protection of specific computers having access control functions from acts of unauthorized computer access.

Penal provisions

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:
i. person who has infringed the provision of Article 3, paragraph 1;
ii. A person who has infringed the provision of Article 6, paragraph 3.

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.

Japan Penal Code - Relevant extracts (contd.)

JURISDICTION

Section 1

Crimes committed at any place inside territory of Japan

1. This Code shall be applicable to everyone who commits any crime at any place inside the territory of Japan.
2. Also, this Code shall be applicable to everyone who commits any crime in Japanese ship or aircraft nevertheless such ship or aircraft is located at any place outside the territory of Japan.

Section 2

Crimes committed at any place outside territory of Japan

This Code shall be applicable to everyone who commits one or over of following crimes at any place outside the territory of Japan.

4 Crimes of Section.154, Section 155, Section 157, Section 158, Section 161-2(concerned with electronic-magnetic records which ought to be produced by State office or public officer).

Section 7-2

Definition of 'electronic-magnetic record'

In this Code, 'electronic-magnetic records' means a record or records which produced by electronic, magnetic or the other human unrecognizable measures, and which are intended to or able to be use to perform information processing in computer system.

Chapter 17. Forgery of Document

Section 161-2 Unlawful production of electronic-magnetic records

1. Any person who intentionally and knowingly, unlawfully, for the purpose to confuse business transactions of others, produce electronic-magnetic records relating to legal rights or duties of others and are being used or intended to be used for such transactions shall be imprisoned at hard labor not more than 5 years or be fined not more than 50,000yen.
2. If the electronic-magnetic records have ought to be produced by State office or public officer, then such person as set forth in previous subsection shall be imprisoned at hard labor not more than 10 years or be fined not more than 100,000yen.
3. Any person who intentionally and knowingly, for the same purpose as set forth in subsection 161.2.1, use unlawfully produced electronic-magnetic records to perform them in business transactions shall be guilty and punishable by penalties as same as applicable to Any person who produces such unlawfully electronic-magnetic records.
4. Any person who attempt to commit any crimes as set forth in this section, shall be punishable.

Chapter 36. Interference with Credit and Transaction

Section 234-2 Interference with business transaction by computer system

Any person who intentionally and knowingly, unlawfully, causes disruption or interference with regular execution of valid performance of computer system which is being used or intended to be use for business transactions of others, or causes executions which are contrary to proper using or purposes of such computer system, by destruction of such computer system or electronic-magnetic records which is being used or intended to use in such computer system, by introducing false information or wrong instructions into such computer system, or by the other similar means, and causes interference with business transactions of others shall be imprisoned at hard labor not more than 5 years or be fined not more than 100,000yen.

Chapter 37. Fraud and Threatening

Section 246-2 Computer Fraud

Any person who intentionally and knowingly, unlawfully, obtain unlawful profit or cause to be obtain unlawful profit to any others, by introducing false information or wrong instructions into computer system which is being used or intended to be use for business transactions of others, by producing false electronic-magnetic records relating to take, loss or change of property of others, or by using such false electronic-magnetic records on any business transactions, shall be imprisoned at hard labor not more than 5 years.

Section 250 Attempt to commit fraud or threatening

Any person who attempt to commit any crimes as set forth in this chapter shall be punishable.

Chapter 40. Damage and Conceal

Section 258 Destruction of official electronic-magnetic records

Any person who destroys any documents or electronic-magnetic records which ought to be use at State office shall be imprisoned at hard labor more than 3 months and not more than 5 years.

Section 259 Destruction of private electronic-magnetic records

Any person who destroys any documents or electronic-magnetic records relating to take, loss or change of property of others shall be imprisoned at hard labor not more than 5 years.

Section 264 Prosecution

Anyone who commit any crimes as set forth in Section 259 or Section 261 shall not be prosecuted without any accusation by victim.

LATVIA

The Criminal Law Section 241:

Arbitrarily Accessing Computer Systems

(1) For a person who commits arbitrarily accessing an automated computer system, if opportunity for an outsider to acquire the information entered into the system is caused thereby, the applicable sentence is custodial arrest, or a fine not exceeding eighty times of monthly wage.

(2) For a person who commits the same acts, if breaching of computer software protective systems or accessing of communications lines is associated therewith, the applicable sentence is deprivation of liberty for a term not exceeding one year, or a fine not exceeding one hundred and fifty times the minimum monthly wage.

LUXEMBOURG

The Act of July 15th, 1993, relating to the reinforcement of the fight against financial crime and computer crime.

Section VI - concerning certain infractions in computer material.

Article 509-1- Whoever fraudulently gains access or supports, wholly or in part, a system of data processing, shall be punished with imprisonment from two months until one year, or a fine from 10.000 to 250.000 F, or both.

The suppression or modification of the data contained in the system, or the alteration of the function of said system, is punishable by imprisonment from two to two years, and a fine from 50.000 to 500.000 F.

MALAYSIA

COMPUTER CRIMES ACT 1997.
PART II
OFFENCES

3 (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.

A person guilty of an offence under this section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment not exceeding five years or to both.

MALTA

CHAPTER 426
ELECTRONIC COMMERCE ACT

AN ACT to provide in relation to electronic commerce and to provide for matters connected therewith or ancillery thereto.

PART VIII
COMPUTER MISUSE

Unlawful access to, or use of, information.

337 (C) (1) A person who without authorisation does any of the folloowing acts shall be guilty of an offence against this article -

(a) uses a computer or any other device or equipment to access any data, software or supporting documentation held in that computer or on any other computer, or uses, copies or modifies any such data, software or supporting documentation;

(b) outputs any data, software or supporting documentation from the computer in which it is held, whether by having it displayed or in any other manner whatsoever;

(c) copies any data, software or supporting documentation to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held;

(d) prevents or hinders access to any data, software or supporting documentation;

(e) impairs the operation of any system, software or the integrity or reliability of any data;

(f) takes possession of or makes use of any data, software or supporting documentation;

(g) installs, moves, alters, erases, destroys, varies or adds to any data, software or supporting documentation;

(h) discloses a password or any other means of access, access code or other access information to any unauthorised person;

(i) uses another person's access code, password, user name, electronic mail addressor other means of access or identification information in a computer;

(j) discloses any data, software or supporting documentation unless this is required in the course of his duties or by any other law.

(2) For the purpose of this Sub-title:

(a) a person shall be deemed to act without authorisation if he is not duly authorised by an entitled person;

(b) a person shall be deemed to be an entitled person if the person himself is entitled to control the activities defined in paragrphs (a) to (j) of subarticle (1) or in paragraphs (a) and (b) of article 4 of this Sub-title.

(3) For the purpose of subarticle (1):

(a) a person shall be deemed to have committed an offence irrespective of whether in the case of any modification, such modification is intended to be permanent or temporary;

(b) the form in which any software or data is output and in particular whether or not it represents a form in which, in the case of software, it is capable of being executed or, in the case of data, it is capable of being processed by a computer, is immaterial.

(4) For the purposes of paragraph (f) of subarticle (1), a person who for the fact that he has in his custody or under his control any data, computer software or supporting documentation which he is not authorised to have, shall be deemed to have taken possession of it.

Offences and Penalties.

337 (F) (1) Without prejudice to any other penalty established under this Sub-title, any person who contravenes any of the provisions of this Sub-title shall be guilty of an offence and shall be liable on conviction to a fine (multa) not exceeding ten thousand liri or to imprisonment for a term not exceeding four years, or to both such fine and imprisonment.

(2) Where any such offence constitutes an act which is in any way detrimental to any function or activity of Government, or hampers, impairs or interrupts in any manner whatsoever the provision of any public service or utility, whether or not such service or utility is provided or operated by any Government entity, the penalty shall be increased to a fine (multa) of not less than one hundred liri and not exceeding fifty thousand liri or to imprisonment for a term from three months to ten years, or both such fine and imprisonment.

MAURITIUS

THE INFORMATION AND COMMUNICATION TECHNOLOGIES BILL

To establish the Information and Communication Technologies Authority, the Information and Communication Technologies Advisory Council, the Information and Communication Technologies Appeal Tribunal and to provide for the regulation and democratisation of information and communication technologies and related matters

33. Data Protection

(1) The Authority shall ensure data protection and security by –

(a) monitoring compliance with the Code of Practice;

(b) conducting a regular review and revision of the Code of Practice;

(c) receiving and advising on complaints of any unlawful or wrongful act; and

(d) carrying out such inspection as may be necessary in relation to personal data held under the Act.

(2) Subject to sub-section (5), every data user or computer service person shall -

(a) upon a written request to that effect being made to the Authority at any reasonable time by an individual; and

(b) upon such request being transmitted by the Authority to such user or person, cause that individual to be informed, without undue delay or expense, whether he holds, or is in possession of, as the case may be, personal data relating to that individual.

(3) Where the Authority so directs, the computer data person shall correct, modify, up-date or delete the personal data relating to any individual.

(4) Any data or computer service person who contravenes subsection (2) shall commit an offence and shall, on conviction, be liable to penal servitude of a term not exceeding 10 years and to a fine not exceeding 1 million rupees.

(5) Subsection (2) shall not apply to any personal data kept for –

(a) safeguarding the State's defence, public safety or public order;

(b) the prevention of crime;

(c) the apprehension or prosecution of offences;

(d) the assessment or collection of any tax or duty;

(e) the following up of the physical or mental health of any individual, where the request is made by a person other than that individual or his next of kin as defined in the Mental Health Care Act 1999;

(f) calculating the amount payable by way of remuneration pension in respect of service in any office or employ;

(g) personal, family or household affairs or recreational purposes; and

(h) determining the results of an academic or other examination.

46. Offences

Any person who -

(a) by any form of emission, radiation, induction or other electromagnetic effect, harms the functioning of an information and communication service,including telecommunication service;

(b) with intent to defraud or to prevent the sending or delivery of a message, takes an information and communication message, including telecommunication message from the employee or agent of a licensee;

(c) with intent to defraud, takes a message from a place or vehicle used by a licensee in the performance of his functions;

(d) steals, secretes or destroys a message;

(e) wilfully or negligently omits or delays the transmission or delivery of a message;

(f) forges a message or transmits or otherwise makes use of a message knowing that it has been forged;

(g) knowingly sends, transmits or causes to be transmitted a false or fraudulent message;

(h) uses an information and communication service, including telecommunication service, -

  (i) for the transmission or reception of a message which is grossly offensive, or of an indecent, obscene or menacing character; or

  (ii) for the purpose of causing annoyance, inconvenience or needless anxiety to any person;

  (iii) for the transmission of a message which is of a nature likely to endanger or compromise State defence, public safety or public order.

(i) dishonestly obtains or makes use of an information and communication service, including telecommunication service with intent to avoid payment of any applicable fee or charge;

(j) by means of an apparatus or device connected to an installation maintained or operated by a licensee -

  (i) defrauds the licensee of any fee or charge properly payable for the use of a service;

  (ii) causes the licensee to provide a service to some other person without payment by such other person of the appropriate fee or charge; or

  (iii) fraudulently installs or causes to be installed an access to a telecommunication line;

(k) wilfully damages, interferes with, removes or destroys an information and communication installation or service including telecommunication installation or service maintained or operated by a licensee;

(l) establishes, maintains or operates a network or service without a licence or in breach of the terms or conditions of a licence;

(m) without the prior approval of the Authority, imports any equipment capable of intercepting a message;

(n) discloses a message or information relating to such a message to any other person otherwise than -

  (i) in accordance with this Act;

  (ii) with the consent of each of the sender of the message and each intended recipient of the message;

  (iii) for the purpose of the administration of justice; or (iv) as authorised by a Judge;

(o) except as expressly permitted by this Act or as authorised by a Judge, intercepts, authorises or permits another person to intercept, or does any act or thing that will enable him or another person to intercept, a message passing over a network;

(p) in any other manner contravenes this Act or any regulations made under this Act, shall commit an offence.

47. Penalties

(1) Any person who commits an offence under this Act shall, on conviction, be liable to a fine not exceeding 1,000,000 rupees and to imprisonment for a term not exceeding 5 years.

(2) The Court before which a person is convicted of an offence under this Act may, in addition to any penalty imposed pursuant to subsection (1), order -

(a) the forfeiture of any installation or apparatus used in connection with the offence;

(b) the cancellation of the licence held by the person convicted;

(c) that the person convicted shall not be issued with a licence for such period as the Court thinks fit;

(d) that a service provided to a person convicted of an offence under this Act shall be suspended for such period as the Court thinks fit.

(3) An offence under this Act shall –

(a) be triable by the Intermediate Court;

(b) not be triable by a District Court.

MEXICO
Penal Code Part 9
Chapter II

Articles 211 bis 1: Whoever without authorization modifies, destroys or causes loss of information contained in computer systems or computer equipments protected by security measures, shall be liable to imprisonment for a term of six months to two years and to fines of one hundre to three hundred days.

Whoever without authorization obtains access to or copies information contained in computer systems or computer equipments protected by security measures, shall be liable to imprisonment for a term of three months to one year and to fines of fifty to one hundred and fifty days.

Articles 211 bis 2: Whoever without authorization modifies, destroys or causes loss of information contained in governmental computer systems or computer equipments protected by security measures, shall be liable to imprisonment for a term of one year to four years and to fines of one hundred to six hundred days.

Whoever without authorization obtains access to or copies information contained in governmental computer systems or equipments protected by security measures, shall be liable to imprisonment for a term of six months to two years and fines of one hundred to three hundred days.

Article 211 bis 4: Whoever without authorization modifies, destroys or causes loss of information contained in computer systems or computer equipments of institutions as part of the financial system protected by security measures, shall be liable to imprisonment for a term of six months to four years and fines of one hundred to six hundred days.

Whoever without authorization obtains access to or copies information contained in computer systems or computer equipments of institutions as part of the financial system protected by security measures, shall be liable to imprisonment for a term of three months to two years and fines of fifty to three hundred days.

THE NETHERLANDS DENMARK

The Danish Criminal Code contains the following provisions that are applicable in relation to computer crime:

(a) Acts causing public damage

§ 193. (1) Any person who, in an unlawful manner, causes major disturbances in the operation of public means of communication, of the public mail service, of publicly used telegraph or telephone services, of radio and television installations, of data processing systems or of installations for the public supply of water, gas, electricity or heating

shall be liable to simple detention or to imprisonment for any term not exceeding four years

or,

in mitigating circumstances, to a fine.

(2) If such an act has been committed through negligence, the penalty shall be a fine or simple detention.

(b) Computer fraud

§ 279 a. Any person who, for the purpose of obtaining for himself or for others an unlawful gain, unlawfully changes, adds or erases information or programs for the use of electronic data processing, or who in any other manner attempts to affect the results of such data processing, shall be guilty of computer fraud.

§ 285. (1) The offences referred to in [i.a. Section 279 a] of this Act [...] shall be punished with imprisonment for any term not exceeding one year and six months.

§ 286. (1) [...]

(2) The penalty for [...] computer fraud [...] may, where the offence is of a particularly aggravated nature or where a large number of such offences have been committed, be increased to imprisonment for any term not exceeding eight years.

(3) [...]

§ 287. (1) If any of the offences dealt with in [i.a. Sections 279 a] of this Act is of minor importance because of the circumstances under which the punishable act was committed, because of the small value of the objects appropriated or of the loss of property sustained or for any other reason,

the penalty shall be a fine. In further mitigating circumstances, the penalty may be remitted.

(2) [...]

(c) Damage to property

§ 291. (1) Any person who destroys, damages or removes objects belonging to others shall be liable to a fine or to simple detention or to imprisonment for any term not exceeding one year.

(2) In the case of very serious damage to property or where the offender has previously been convicted under this Section or in pursuance of Sections 180, 181, 183 (1) or (2), 184 (1), 193 or 194 of this Act, the penalty may be increased to imprisonment for any term not exceeding four years.

(3) Where the damage has been done through gross negligence in the circumstances referred to in Subsection (2) above, the penalty shall be a fine or simple detention or imprisonment for any term not exceeding six months

NEW ZEALAND

No special penal legislation, but
The Crimes Amendment (No 6) Bill is pending in the Parliament. This Bill includes sections on Crimes Involving Computers:

Section 305ZD:	Interpretation
Section 305ZE:	Accessing computer system for dishonest purpose.
Section 305ZF:	Damaging or interfering with computer system.
Section 305FA:	Accessing computer system without authorisation

NORWAY

Penal Code § 145:

Any person who unlawfully opens a letter or other closed document or in a similar manner gains access to its contents, or who breaks into another persons locked depository shall be liable to fines or to imprisonment for a term not exceeding 6 months.

The same penalty shall apply to any person who by breaking a protective device or in a similar manner, unlawfully obtains access to data or programs which are stored or transferred by electronic or other technical means.

If damage is caused by the acquisition or use of such unauthorized knowledge, or if the felony is committed for the purpose of obtaining for any person an unlawful gain, imprisonment for a term not exceeding 2 years may be imposed.

Accomplices shall be liable to the same penalty. Public prosecution will only be instituted when the public interest so requires.

Penal Code § 151 b:

Any person who by destroying, damaging, or putting out of action any data collection or any installation for supplying power, broadcasting, telecommunication, or transport causes comprehensive disturbance in the public administration or in community life in general shall be liable to imprisonment for a term not exceeding 10 years.

Negligent acts of the kind mentioned in the first paragraph shall be punishable by fines or imprisonment for a term not exceeding one year.

Accomplices shall be liable to the same penalty.

Penal Code § 261:

Any person who unlawfully uses or disposes of any chattel that belongs to another person and thereby obtains for himself or another a considerable gain, or inflicts on the person entitled thereto a considerable loss, shall be liable to imprisonment for a term not exceeding three years. The penalty for aiding and abetting is the same. Under especially extenuating circumstances fines may be imposed.

A public prosecution will only be instituted when requested by the aggrieved person unless it is required in the public interest.

Penal Code § 291:

Any person who unlawfully destroys, damages, renders useless or wastes an object that wholly or partly belongs to another shall be guilty of vandalism.

The penalty for vandalism shall be fines or imprisonment for a term not exceeding one year. An accomplice shall be liable to same penalty.

A public prosecution will only be instituted when requested by the aggrieved person unless it is required in the public interest.

POLAND

The Code expressly prohibits acts specified in the following provisions:

Article 130,

Section 3 of the Code (concerning espionage): entailing, among other things, the act of connecting to a computer network:

Article 130.

Section 3. Who in order to provide information specified in Section 2 to a foreign intelligence service gathers and stores such information, connects to a computer network in order to obtain such information, or declares his/her willingness to act for the benefit of a foreign intelligence service against the Republic of Poland shall be subject to imprisonment for a period from six months to eight years.

Article 165,

Section 1: Who imperils the life or health of a great number of people or property of great value:

Section 4: by interfering with, disabling, or otherwise affecting the automatic processing, gathering, or transfer of information shall be subject to imprisonment for a period from six months to eight years

Article 268,

Section 1: Who without authorization destroys, damages, removes, or changes the records of important information, or otherwise prevents the authorized person from reading such information or significantly impedes the process shall be subject to restriction of liberty or imprisonment for a period of up to two years.

Section 2: If the act specified in Section 1 concerns records on a computer information carrier, the perpetrator shall be subject to imprisonment for a period of up to three years.

Section 3: Who in committing the act specified in Sections 1 or 2 causes substantial damage to property shall be subject to restriction of liberty for a period from three months to five years.

Article 278,

Section 1: Who takes possession of someone else's movable thing in order to appropriate it shall be subject to imprisonment for a period from three months up to five years.

Section 2: The same penalty shall apply to the person who without the consent of the authorized person obtains someone else's computer program in order to benefit.

An additional area of protection covers the provisions of the General Inspector for Personal Data Protection Act. The standards set in the Act are in principle common with those in other countries affiliated with the Council of Europe.

The Act includes the following criminal provisions:

Chapter 8
Criminal provisions
Article 49.

Section 1. Who without permission or authorization processes personal data in a file shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to two years.

Section 2. If the act specified in Section 1 concerns data which discloses racial or ethnic background, political views, religious or philosophical beliefs, denomination, party or trade union membership, information on the state of health, genetic code, addictions, or sexual life, the perpetrator shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to three years.

Article 50.

Section 1. Who in administering a data file stores in a file personal data conflicting with the purpose for which the file was created, shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to one year.

Article 51

Section 1. Who in administering a data file or being obliged to protect personal data makes it available or grants access to such data to unauthorized persons shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to two years.

Section 2. If the perpetrator's act is unintentional, he/she shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to one year.

Article 52

Who in administering data violates, even unintentionally, the obligation to protect such data against theft by an unauthorized person, damage, or destruction shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to one year.

Article 53

Where a person who is obligated to submit a data file for registration fails to do so, he/she shall be subject to restriction of liberty or imprisonment for a period of up to one year.

Article 54

Who in administering a data file fails to observe the obligation to notify the data subject about his/her rights or to pass to that person information that enables the person under consideration to exercise his/her rights under the Act shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to one year.

Additionally, in connection with the said Act we have in force Regulation of the Minister of Internal Affairs and Administration dated June 3, 1998 on setting the basic technical and organization specifications to be met by IT equipment and systems serving for the purposes of personal data processing *(Dziennik Ustaw No 80 (1998),* Item 521). The Regulation does not include criminal provisions.

PORTUGAL

Criminal Information Law of August 17, 1991:
Chapter 1 Article 7:

1 Any person who, without authorization obtains for himself or another person an unlawful gain or use by any manner accessing an information system or network, shall be sentenced to imprisonment not exceeding one year, or to a fine and imprisonment not exceeding 120 days.

2 Imprisonment not exceeding three years or a fine if the person concerned obtains access to information by breaking the security rules.

3 Imprisonment for a term of one year not exceeding five years when:

(a) the person concerned by obtaining access to information acquires knowledge of trade secrets or confidential data protected by law,

(b) the gain or use results in comprehensive values.

REPUBLIC OF THE PHILIPPINES
Republic Act No. 8792

AN ACT PROVIDING FOR THE RECOGNITION AND USE OF ELECTRONIC COMMERCIAL AND NON - COMMERCIAL TRANSACTIONS AND DOCUMENTS, PENALTIES FOR UNLAWFUL USE THEREOF AND FOR OTHER PURPOSES

SEC. 31. Lawful Access.

Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plaintext, electronic signature or file and solely for the authorized purposes. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key.

SEC. 32. Obligation of Confidentiality.

Except for the purposes authorized under this Act, any person who obtained access to any electronic key, electronic data message, or electronic document, book, register, correspondence, information, or other material pursuant to any powers conferred under this Act, shall not convey to or share the same with any other person.

SEC. 33. Penalties.

The following Acts shall be penalized by fine and/or imprisonment, as follows:

a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

b) Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

c) Violations of the Consumer Act or Republic Act No. 7394 and other relevant or pertinent laws through transactions covered by or using electronic data messages or electronic documents, shall be penalized with the same penalties as provided in those laws;

d) Other violations of the provisions of this Act, shall be penalized with a maximum penalty of one million pesos (P1,000,000.00) or six (6) years imprisonment.

The Act includes the following criminal provisions:

Chapter 8

Criminal provisions

Article 49.

Section 1. Who without permission or authorization processes personal data in a file shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to two years.

Section 2. If the act specified in Section 1 concerns data which discloses racial or ethnic background, political views, religious or philosophical beliefs, denomination, party or trade union membership, information on the state of health, genetic code, addictions, or sexual life, the perpetrator shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to three years.

Article 50.

Section 1. Who in administering a data file stores in a file personal data conflicting with the purpose for which the file was created, shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to one year.

Article 51

Section 1. Who in administering a data file or being obliged to protect personal data makes it available or grants access to such data to unauthorized persons shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to two years.

Section 2. If the perpetrator's act is unintentional, he/she shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to one year.

Article 52

Who in administering data violates, even unintentionally, the obligation to protect such data against theft by an unauthorized person, damage, or destruction shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to one year.

Article 53

Where a person who is obligated to submit a data file for registration fails to do so, he/she shall be subject to restriction of liberty or imprisonment for a period of up to one year.

Article 54

Who in administering a data file fails to observe the obligation to notify the data subject about his/her rights or to pass to that person information that enables the person under consideration to exercise his/her rights under the Act shall be subject to a fine, restriction of liberty, or imprisonment for a period of up to one year.

Additionally, in connection with the said Act we have in force Regulation of the Minister of Internal Affairs and Administration dated June 3, 1998 on setting the basic technical and organization specifications to be met by IT equipment and systems serving for the purposes of personal data processing (*Dziennik Ustaw No 80 (1998),* Item 521). The Regulation does not include criminal provisions.

SOUTH AFRICA

THE ELECTRONIC COMMUNICATIONS AND TRANSACTIONS ACT of July 31 2002 (Act No. 25, 2002)
CHAPTER XIII
CYBER CRIME

Unauthorised 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 utilise such item to contravene this section, is guilty of an offence.

(4) A person who utilises 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.

SPAIN :

CHAPTER I
On the discovery and revealing of secrets

Article 197.

1. Any individual who, for the purpose of discovering the secrets or violating the privacy of another and without the consent of the latter, takes possession of that individual's papers, letters, electronic mail messages or any other personal documents or belongings or intercepts his or her telecommunications or uses technical devices for listening, transmitting, recording or reproducing sound or images or any other communications signal, will be punished by imprisonment from between one and four years and a fine of between twelve and twenty-four months .
2. The same punishment will be applicable to any individual who, without authorization, seizes, uses or modifies, to the detriment of a third party, such private personal or family data of another individual as may be recorded on computer, electronic or telematic files or media, or in any other type of file or record, whether public or private. The same punishment will be imposed on any individual who, without authority, accesses such data by any means or alters or uses such data to the detriment of the owner of the data or of a third party.
3. Punishment consisting of imprisonment from between two and five years will be imposed if the data or facts discovered or the images captured, as indicated in the proceeding paragraphs, are divulged, revealed or transferred to third parties. Punishment consisting of imprisonment from between one and three years and a fine of between twelve and twenty-four months will be imposed on any individual who, with prior knowledge of the illicit origin of [such facts or data] [but] without having taken part in their discovery, commits the acts described in the preceding paragraph.
4. If the acts described in paragraphs 1 and 2 of this article are committed by the persons in charge of or responsible for the computer, electronic or telematic files and media or files or records, punishment consisting of imprisonment from between three and five years will be imposed, and if such private data are disseminated, transferred or made public, the upper half of the punishment will be imposed.
5. In addition, when the acts described in the above sections involve personal data revealing the ideology, religion, beliefs, health, racial origin or sexual orientation, or if the victim is a minor or incapacitated, the upper half of the punishments stipulated will be imposed.
6. If such acts are committed with intent to profit, the upper half of the punishments set forth respectively in paragraphs 1 through 4 of this article will be imposed. If in addition they involve the data mentioned in paragraph 5, the punishment will consist of imprisonment from between four and seven years.

SECTION 1. ON FRAUD

Article 248.

1. Any individual will be guilty of fraud who, with intent to profit, uses sufficient deceit to cause another individual to err, inducing him or her to commit an act of disposition to the detriment of him or herself or a third party.

2. Also guilty of fraud will be any individual who, with intent to profit and using computer manipulation or any similar contrivance, causes the unauthorized transfer of any personal asset to the detriment of a third party.

Article 264.

1. Punishment consisting of imprisonment from between one and three years and a fine of between twelve and twenty-four months will be imposed on any individual who causes the injury identified in the preceding article in any of the following circumstances:
    1. The acts are committed for the purpose of preventing the free exercise of authority or in vengeance therefor, whether the crime is committed against public authorities or against private citizens who, whether acting as witnesses or in any other capacity, have contributed, or might in the future contribute, to the execution or application of the Law or General Provisions.
    2. Infection or contagion of cattle is caused by any means.
    3. Poisonous or corrosive substances are used.
    4. Assets in the public or community domain or assets designated for public or community use are involved.
    5. The acts lead to the bankruptcy of the individual affected or place him or her in a grave economic situation.
2. The same punishment will be imposed on any individual who, in any way, destroys, modifies, misuses or otherwise damages such electronic data, programs or documents of others as may be contained in computer networks, media or systems.

Article 256.

Any individual who makes use of any telecommunications terminal equipment without the consent of the owner thereof, causing damage to the latter in excess of fifty thousand pesetas, will be subject to punishment consisting of a fine of between three and twelve months .

Article 270.

Punishment consisting of imprisonment from between six months and two years or a fine of between six and twenty-four months will be imposed on any individual who, with intent to profit and to the detriment of a third party, reproduces, plagiarizes, distributes or publicly communicates, either wholly or in part, a literary, artistic or scientific work or the transformation, interpretation or artistic execution thereof contained in any medium or communicated by any means, without the authorization of the holders of the corresponding intellectual property rights or successors thereof.

The same punishment will be imposed on any individual who intentionally imports, exports or stores copies of such works or productions or executions without the authorization specified above.

The same punishment will be imposed in the event of the manufacture, circulation and possession of any medium specifically designed to facilitate the unauthorized suppression and neutralization of any technical device used to protect computer programs.

SECTION 2. ON CRIMES INVOLVING INDUSTRIAL PROPERTY

Article 273.

1. Punishment consisting of imprisonment from between six months and two years and a fine of between six and twenty-four months will be imposed on any individual who, for

industrial or commercial purposes, without the consent of the owner of a patent or utility model, and with prior knowledge of its registration, manufactures, imports, possesses, utilizes, offers or introduces into the market items covered by such rights.

2. The same punishment will be imposed on any individual who, in the same fashion and for the above-indicated purposes, uses or offers the use of a procedure covered by a patent, or who possesses, offers, introduces into the market or uses the product directly obtained by the patented procedure.
3. The same punishment will be imposed on any individual who commits any of the acts characterized in the first paragraph of this article, under identical circumstances, with regard to objects covered in favor of a third party by an industrial or artistic model or drawing or topography of a semiconductor product.

SWEDEN

Penal Code Chapter 4, Section 9 c:

A Person who, in cases other than than those defined in Section 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for breach of data secrecy to a fine or imprisonment for at most two years., unless the deed is criminalized in the Criminal Code or in the 1990 Protection of Trade Secrets Act. A recording in this context includes even information that is being processed by electronic or similar means for use with automatic data processing. (Law 1998:206)

Attempt and preparation shall be punished as stated in Chapter 23 of the Criminal Code, unless the completed crime would have been regarded as a petty.

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.

Comparative Study of US LAWS and the IT ACT 2000.

18 U.S.C. 1029.
Fraud and Related Activity in Connection with Access Devices

Fraud and related activity in connection with access devices

(a) Whoever--

i. knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
ii. knowingly and with intent to defraud traffics in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;
iii. knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
iv. knowingly, and with intent to defraud, produces, traffics in, has control or custody of, or possesses device-making equipment;
v. knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment or any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;
vi. without the authorization of the issuer of the access device, knowingly and with intent to defraud solicits a person for the purpose of—
    a. offering an access device; or
    b. selling information regarding or an application to obtain an access device;
vii. knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

1. Similar penal sections are there in the Indian penal Code, not specifically but in the broad category of Frauds and Cheating.
2. Fraudulent charging of time made an offence in IT ACT 2000.

viii. knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

ix. knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

x. without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, 1 or more evidences or records of transactions made by an access device; shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

(b)

i. Whoever attempts to commit an offense under subsection (a) of this section shall be subject to the same penalties as those prescribed for the offense attempted.

ii. Whoever is a party to a conspiracy of two or more persons to commit an offense under subsection (a) of this section, if any of the parties engages in any conduct in furtherance of such offense, shall be fined an amount not greater than the amount provided as the maximum fine for such offense under subsection (c) of this section or imprisoned not longer than one-half the period provided as the maximum imprisonment for such offense under subsection (c) of this section, or both.

(c) Penalties.--

i. Generally.--The punishment for an offense under subsection (a) of this section is.—

a. in the case of an offense that does

not occur after a conviction for another offense under this section.—

i. if the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and
ii. if the offense is under paragraph (4), (5), (8), or (9), of subsection (a), a fine under this title or imprisonment for not more than 15 years, or both;

b. in the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and
c. in either case, forfeiture to the United States of any personal property used or intended to be used to commit the offence.

Forfeiture procedure.--The forfeiture of property under this section, including any seizure and disposition of the property and any related administrative and judicial proceeding, shall be governed by section 413 of the Controlled Substances Act, except for subsection (d) of that section.

The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Such authority of the United States Secret Service shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

18 U.S.C. 1030.Fraud and Related Activity in Connection with Computers

Fraud and Related Activity in Connection with Computers

(a) Whoever

i. 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

1. Adequately addressed to in IT Act under the heading Hacking, and other penal sections of IT Act 2000.
2. The Law is salient on Data under in transit. This could be incorporated but substitution or by adequately redefining "Data" to include Data in Transit"
3. Need to define "protected System", and frame rules.

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;

ii. 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 U.S.C. 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;

iii 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;

iv 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 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) (A) 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;	Adequately addressed
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	Need to define "protected System"
(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 $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;	No specific offence under Indian Laws
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;	Adequately covered
(7) a. 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; b. shall be punished as provided in subsection (c) of this section. c. (b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section. d. (c) The punishment for an offense under subsection (a) or (b) of this section is -- (1) a. a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and b. a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and (2) a. except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this	

section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

b. a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2)or an attempt to commit an offense punishable under this subparagraph, if-
   i. the offense was committed for purposes of commercial advantage or private financial gain;
   ii. the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
   iii. the value of the information obtained exceeds $5,000;

c. a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(3)

a. a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4), or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

b. a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii) or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(4)

a. a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

b. a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

c. a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

d. (1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

CBI to be made a nodal agency and Certain Crimes as recommended by Maliamath Committee be classified as "Federal Crimes"

18 U.S.C. 1362. Communication Lines, Stations, or Systems

§1362. Communication lines, stations, or systems Whoever wilfully or maliciously injures or destroys or attempts wilfully or maliciously to injure or destroy any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defence functions of the United States, whether constructed or in process of construction, or wilfully or maliciously interferes in any way with the working or use of any such line, or system, or wilfully or maliciously obstructs, hinders, or delays the transmission of any communication over any such line, or system, shall be fined under this title or imprisoned not more than ten years, or both. In the case of any works, property, or material, not operated or controlled by the United States, this section shall not apply to any lawful strike activity, or other lawful concerted activities for the purposes of collective bargaining or other mutual aid and protection which do not injure or destroy any line or system used or intended to be used for the military or civil defence functions of the United States.	Adequately addressed.

18 U.S.C. 2511. Interception and Disclosure of Wire, Oral, or Electronic Communications Prohibited

§ 2511. Interception and disclosure of wire, oral, or electronic communications prohibited (1) Except as otherwise specifically provided in this chapter any person who– a. intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; b. intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept	Adequate provisions for forcing disclosure of information exist under IT Act. 1. However with evolving techniques for hiding information, the provision should not be restricted to Encryptions only. It should be generic to include other techniques such as steganography, digital water marking etc also. 2. A comprehensive Encryption policy should also be evolved. 3. Powers to sanction interception is vested

any oral communication when--

i. such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
ii. such device transmits communications by radio, or interferes with the transmission of such communication; or
iii. such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
iv. such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
v. such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States;

c. intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;

d. intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or

e.

i. intentionally discloses, or endeavors

with different authorities presently, under the various laws. It is recommended that this issue be resolved early, specially because of the convergence of communication technologies. The power should rest in on authority only.

to disclose, to any other person the contents of any wire, oral, or electronic communication, intercepted by means authorized by sections 2511(2)(a)(ii), 2511(2)(b) to (c), 2511(2)(e), 2516, and 2518 of this chapter,

ii. knowing or having reason to know that the information was obtained through the interception of such a communication in connection with a criminal investigation,

iii. having obtained or received the information in connection with a criminal investigation, and

iv. with intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation, shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)

(A)

i. It shall not be unlawful under this chapter for an operator of a switchboard, or on officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

ii. Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

(a) a court order directing such assistance signed by the authorizing judge, or

(b) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required, setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order or certification under this chapter.

(b)

It shall not be unlawful under this chapter for an officer, employee, or agent of the Federal Communications Commission, in the normal course of his employment and in discharge of the monitoring responsibilities exercised by the Commission in the enforcement of chapter 5 of title 47 of the United States Code, to intercept a wire or electronic communication, or oral communication transmitted by radio, or to disclose or use the information thereby obtained.

(c)

It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception.

(d)

It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

(e)

Notwithstanding any other provision of this title or section 705 or 706 of the Communications Act of 1934, it shall not be unlawful for an officer, employee, or agent of the United States in the normal course of his official duty to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, as authorized by that Act.

(f)

Nothing contained in this chapter or chapter 121, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire and oral communications may be conducted.

(g)

It shall not be unlawful under this chapter or chapter 121 of this title for any person—

i. to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public;
ii. to intercept any radio communication which is transmitted--
    a. by any station for the use of the general public, or that relates to ships, aircraft, vehicles, or persons in distress;
    b. by any governmental, law enforcement, civil defense, private land mobile, or public safety communications system, including police and fire, readily accessible to the general public;
    c. by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band, or general mobile radio services; or
    d. by any marine or aeronautical communications system;
iii. to engage in any conduct which--
    (I) is prohibited by section 633 of the Communications Act of 1934; or
    (II) is excepted from the application of section 705(a) of the Communications Act of 1934 by section 705(b) of that Act;
iv. to intercept any wire or electronic

communication the transmission of which is causing harmful interference to any lawfully operating station or consumer electronic equipment, to the extent necessary to identify the source of such interference; or

v. for other users of the same frequency to intercept any radio communication made through a system that utilizes frequencies monitored by individuals engaged in the provision or the use of such system, if such communication is not scrambled or encrypted.

(h) It shall not be unlawful under this chapter

i. to use a pen register or a trap and trace device (as those terms are defined for the purposes of chapter 206 (relating to pen registers and trap and trace devices) of this title); or

ii. for a provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of such service.

(3)

a. Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

b. A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

i. as otherwise authorized in section 2511(2)(a) or 2517 of this title;

ii. with the lawful consent of the originator or any addressee or intended recipient of such communication;

iii. to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

iv. which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

(4)

a. Except as provided in paragraph (b) of this subsection or in subsection (5), whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both.

b. If the offense is a first offense under paragraph (a) of this subsection and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, and the wire or electronic communication with respect to which the offense under paragraph (a) is a radio communication that is not scrambled, encrypted, or transmitted using modulation techniques the essential parameters of which have been withheld from the public with the intention of preserving the privacy of such communication, then--

i. if the communication is not the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, and the conduct is not that described in subsection (5), the offender shall be fined under this title or imprisoned not more than one year, or both; and

ii. if the communication is the radio portion of a cellular telephone communication, a cordless telephone communication that is transmitted between the cordless telephone handset and the base unit, a public land mobile radio service communication or a paging service communication, the offender shall be fined under this title.

c Conduct otherwise an offense under this subsection that consists of or relates to the interception of a satellite transmission that is not encrypted or scrambled and that is transmitted--

i. to a broadcasting station for purposes of retransmission to the general public; or

ii. as an audio subcarrier intended for redistribution to facilities open to the public, but not including data transmissions or telephone calls, is not an offense under this subsection unless the conduct is for the purposes of direct or indirect commercial advantage or private financial gain.

(5)

(a)

i. If the communication is--

a. a private satellite video communication that is not scrambled or encrypted and the conduct in violation of this chapter is the private viewing of that communication and is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain; or

b. a radio communication that is transmitted on frequencies allocated under subpart D of part 74 of the rules of the Federal Communications Commission that is not scrambled or encrypted and the conduct in violation of this chapter is not for a tortious or illegal purpose or for purposes of direct or indirect commercial advantage or private commercial gain, then the person who engages in such conduct shall be subject to suit by the Federal Government in a court of competent jurisdiction.

ii. in an action under this subsection--

a. if the violation of this chapter is a first offense for the person under paragraph (a) of subsection (4) and such person has not been found liable in a civil action under section 2520 of this title, the Federal Government shall be entitled to appropriate injunctive relief; and

b. if the violation of this chapter is a second or subsequent offense under paragraph (a) of subsection (4) or such person has been found liable in any prior civil action under section 2520, the person shall be subject to a mandatory $500 civil fine.

The court may use any means within its authority to enforce an injunction issued under paragraph (ii)(A), and shall impose a civil fine of not less than $500 for each violation of such an injunction.

18 U.S.C. 2701. Unlawful Access to Stored Communications

§ 2701. Unlawful Access to Stored Communications

a. Offense.--Except as provided in subsection (c) of this section whoever–

Adequately addressed by IT Act and IPC

   i. intentionally accesses without authorization a facility through which an electronic communication service is provided; or
   ii. intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

b.

Punishment.--The punishment for an offense under subsection (a) of this section is–

   i. if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain--
      a. a fine under this title or imprisonment for not more than one year, or both, in the case of a first offense under this subparagraph; and
      b. a fine under this title or imprisonment for not more than two years, or both, for any subsequent offense under this subparagraph; and

ii. a fine under this title or imprisonment for not more than six months, or both, in any other case.

c.

Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized–

i. by the person or entity providing a wire or electronic communications service;

ii. by a user of that service with respect to a communication of or intended for that user; or

iii. in section 2703, 2704 or 2518 of this title.

18 U.S.C. 2702. Disclosure of Contents

§ 2702. Disclosure of Contents

a. Prohibitions.--Except as provided in subsection (b)—

1. a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

2 a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

   a. on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; and

   b. solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

3 a provider of remote computing service

The provisions pertain to Data Secrecy. We do not have a comprehensive exclusive law on this issue. The provisions are addressed to by invoking various laws, rules, and regulations.

With India becoming a leading choice for outsourcing, a separate "Data Protection Act" may be framed, to address this issue especially for the Private sector.

or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

b. Exceptions.--A person or entity may divulge the contents of a communication–

   i. to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;
   ii. as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;
   ii. with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;
   iv. to a person employed or authorized or whose facilities are used to forward such communication to its destination;
   v. as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service; or
   vi. to a law enforcement agency--

      a. if the contents--

      (i) were inadvertently obtained by the service provider; and

      (ii) appear to pertain to the commission of a crime; or

      b. if required by section 227 of the Crime Control Act of 1990 [42 U.S.C.A. S 13032].

      c. if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay.

(c) Exceptions for disclosure of customer records. A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

   i. as otherwise authorized in section 2703;
   ii. with the lawful consent of the customer or

subscriber;

iii, as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

iv. to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

v. to any person other than a governmental entity.

18 U.S.C. 2703. Requirements for Governmental Access

§ 2703. Requirements for Governmental Access

a. Contents of electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of an electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of an electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Contents of electronic communications in a remote computing service.--

   i. A governmental entity may require a provider of remote computing service to disclose the contents of any electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection–

      a. without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures

No such provision exists in India for Service Providers.

1. There is a need to incorporate similar rules in their service contract.
2. There is a need to spell out the obligations of ISP's in the IT Act 2000.

described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

b. with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

   i. uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

   ii. obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

ii. Paragraph (1) is applicable with respect to any electronic communication that is held or maintained on that service–

   a. on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

   b. solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. Records concerning electronic communication service or remote computing service.--

   i. A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

a. obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
b. obtains a court order for such disclosure under subsection (d) of this section;
c. has the consent of the subscriber or customer to such disclosure; or
d. submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
e. seeks information under paragraph (2).

ii. A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

a. name;
b. address;
c. local and long distance telephone connection records, or records of session times and durations;
d. length of service (including start date) and types of service utilized;
e. telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
f. means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or

State grand jury or trial subpoena or any means available under paragraph (1).

iii. A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

d. Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction described in section 3127(2)(A) and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

e. No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, or certification under this chapter.

f. Requirement to preserve evidence.--

   i. In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

ii. Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

COMMENTS ON THE PATRIOT ACT 2001 USA

Section 202 Authority to Intercept Voice Communications in Computer Hacking Investigations

Previous law: Under previous law, investigators could not obtain a wiretap order to intercept wire communications (those involving the human voice) for violations of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). For example, in several investigations, hackers have stolen teleconferencing services from a telephone company and used this mode of communication to plan and execute hacking attacks.

Amendment: Section 202 amends 18 U.S.C. § 2516(1) – the subsection that lists those crimes for which investigators may obtain a wiretap order for wire communications – by adding felony violations of 18 U.S.C. § 1030 to the list of predicate offenses.1 This provision will sunset December 31, 2005.

Section 209 Obtaining Voice-mail and Other Stored Voice Communications

Previous law: Under previous law, the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 et seq., governed law enforcement access to stored electronic communications (such as e-mail), but not stored wire communications (such as voice-mail). Instead, the wiretap statute governed such access because the definition of "wire communication" (18 U.S.C. § 2510(1)) included stored communications, arguably requiring law enforcement to use a wiretap order (rather than a search warrant) to obtain unopened voice communications. Thus, law enforcement authorities used a wiretap order to obtain voice communications stored with a third party provider but could use a search warrant if that same information were stored on an answering machine inside a criminal's home.

Regulating stored wire communications through section 2510(1) created large and unnecessary burdens for criminal investigations. Stored voice communications possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable.

Moreover, in large part, the statutory framework envisions a world in which technology-mediated voice communications (such as telephone calls) are conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress acknowledged that data and voice might co-exist in a single transaction, it did not anticipate the convergence of these two kinds of communications typical of today's telecommunications networks. With the advent of MIME — Multipurpose Internet Mail Extensions — and similar features, an e-mail may include one or more "attachments" consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect's unopened e-mail from an ISP by means of a search warrant (as required under 18 U.S.C. § 2703(a)) had no way of knowing whether the inbox messages include voice attachments (i.e., wire communications) which could not be compelled using a search warrant.

Amendment: Section 209 of the Act alters the way in which the wiretap statute and ECPA apply to stored voice communications.2 The amendments delete "electronic storage" of wire communications from the definition of "wire communication" in section 2510 and insert language in section 2703 to ensure that stored wire communications are covered under the same rules as stored electronic communications. Thus, law enforcement can now obtain such communications using the procedures set out in section 2703 (such as a search warrant), rather than those in the wiretap statute (such as a wiretap order).

This provision will sunset December 31, 2005.

Section 210 Scope of Subpoenas for Electronic Evidence

Previous law: Subsection2703(c) allows the government to use a subpoena to compel a limited class of information, such as the customer's name, address, length of service, and means of payment. Prior to the amendments in Section 210 of the Act, however, the list of records that investigators could obtain with a subpoena did not include certain records (such as credit card number or other form of payment for the communication service) relevant to determining a customer's true identity. In many cases, users register with Internet service providers using false names. In order to hold these individuals responsible for criminal acts committed online, the method of payment is an essential means of determining true identity.

Moreover, many of the definitions in section 2703(c) were technology-specific, relating primarily to telephone communications. For example, the list included "local and long distance telephone toll billing records," but did not include parallel terms for communications on computer networks, such as "records of session times and durations." Similarly, the previous list allowed the government to use a subpoena to obtain the customer's "telephone number or other subscriber number or identity," but did not define what that phrase meant in the context of Internet communications.

Amendment: Amendments to section 2703(c) update and expand the narrow list of records that law enforcement authorities may obtain with a subpoena. The new subsection 2703(c)(2) includes "records of session times and durations," as well as "any temporarily assigned network address." In the Internet context, such records include the Internet Protocol (IP) address assigned by the provider to the customer or subscriber for a particular session, as well as the remote IP address from which a customer connects to the provider. Obtaining such records will make the process of identifying computer criminals and tracing their Internet communications faster and easier.

Moreover, the amendments clarify that investigators may use a subpoena to obtain the "means and source of payment" that a customer uses to pay for his or her account with a communications provider, "including any credit card or bank account number." 18 U.S.C. §2703(c)(2)(F). While generally helpful, this information will prove particularly valuable in identifying the users of Internet services where a company does not verify its users' biographical information. (This section is not subject to the sunset provision in section 224 of the Act).

Section 211 Clarifying the Scope of the Cable Act

Previous law: The law contains two different sets of rules regarding privacy protection of communications and their disclosure to law enforcement: one governing cable service (the "Cable Act") (47 U.S.C. § 551), and the other applying to the use of telephone service and Internet access (the wiretap statute, 18 U.S.C. § 2510 et seq.; ECPA, 18 U.S.C. § 2701 et seq.;

and the pen register and trap and trace statute (the "pen/trap" statute), 18 U.S.C. § 3121 et seq.).

Prior to the amendments in Section 211 of the Act, the Cable Act set out an extremely restrictive system of rules governing law enforcement access to most records possessed by a cable company. For example, the Cable Act did not allow the use of subpoenas or even search warrants to obtain such records. Instead, the cable company had to provide prior notice to the customer (even if he or she were the target of the investigation), and the government had to allow the customer to appear in court with an attorney and then justify to the court the investigative need to obtain the records. The court could then order disclosure of the records only if it found by "clear and convincing evidence" – a standard greater than probable cause or even a preponderance of the evidence – that the subscriber was "reasonably suspected" of engaging in criminal activity. This procedure was completely unworkable for virtually any criminal investigation.

The legal regime created by the Cable Act caused grave difficulties in criminal investigations because today, unlike in 1984 when Congress passed the Cable Act, many cable companies offer not only traditional cable programming services but also Internet access and telephone service. In recent years, some cable companies have refused to accept subpoenas and court orders pursuant to the pen/trap statute and ECPA, noting the seeming inconsistency of these statutes with the Cable Act's harsh restrictions. See In re Application of United States, 36 F. Supp. 2d 430 (D. Mass. Feb. 9, 1999) (noting apparent statutory conflict and ultimately granting application for order under 18 U.S.C. 2703(d) for records from cable company providing Internet service). Treating identical records differently depending on the technology used to access the Internet made little sense. Moreover, these complications at times delayed or ended important investigations.

Amendment: Section 211 of the Act amends title 47, section 551(c)(2)(D), to clarify that ECPA, the wiretap statute, and the trap and trace statute govern disclosures by cable companies that relate to the provision of communication services – such as telephone and Internet services. The amendment preserves, however, the Cable Act's primacy with respect to records revealing what ordinary cable television programing a customer chooses to purchase, such as particular premium channels or "pay per view" shows. Thus, in a case where a customer receives both Internet access and conventional cable television service from a single cable provider, a government entity can use legal process under ECPA to compel the provider to disclose only those customer records relating to Internet service. (This section is not subject to the sunset provision in Section 224 of the Act).

Section 212 Emergency Disclosures by Communications Providers

Previous law: Previous law relating to voluntary disclosures by communication service providers was inadequate in two respects. First, it contained no special provision allowing providers to disclose customer records or communications in emergencies. If, for example, an Internet service provider ("ISP") independently learned that one of its customers was part of a conspiracy to commit an imminent terrorist attack, prompt disclosure of the account information to law enforcement could save lives. Since providing this information did not fall within one of the statutory exceptions, however, an ISP making such a disclosure could be sued civilly.

Second, prior to the Act, the law did not expressly permit a provider to voluntarily disclose non-content records (such as a subscriber's login records) to law enforcement for purposes of self-protection, even though providers could disclose the content of communications for this reason. See 18 U.S.C. § 2702(b)(5), 2703(c)(1)(B). Yet the right to disclose the content of communications necessarily implies the less intrusive ability to disclose non-content records. Cf. United States v. Auler, 539 F.2d 642, 646 n.9 (7th Cir. 1976) (phone company's authority to monitor and disclose conversations to protect against fraud necessarily implies right to commit lesser invasion of using, and disclosing fruits of, pen register device) (citing United States v. Freeman, 524 F.2d 337, 341 (7th Cir. 1975)). Moreover, as a practical matter, providers must have the right to disclose to law enforcement the facts surrounding attacks on their systems. For example, when an ISP's customer hacks into the ISP's network, gains complete control over an e-mail server, and reads or modifies the e-mail of other customers, the provider must have the legal ability to report the complete details of the crime to law enforcement.

Amendment: Section 212 corrects both of these inadequacies in previous law. Section 212 amends subsection 2702(b)(6) to permit, but not require, a service provider to disclose to law enforcement either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. This voluntary disclosure, however, does not create an affirmative obligation to review customer communications in search of such imminent dangers.

The amendments in Section 212 of the Act also change ECPA to allow providers to disclose information to protect their rights and property. It accomplishes this change by two related sets of amendments. First, amendments to sections 2702 and 2703 of title 18 simplify the treatment of voluntary disclosures by providers by moving all such provisions to 2702. Thus, section 2702 now regulates all permissive disclosures (of content and non-content records alike), while section 2703 covers only compulsory disclosures by providers. Second, an amendment to new subsection 2702(c)(3) clarifies that service providers do have the statutory authority to disclose non-content records to protect their rights and property. All of these changes will sunset December 31, 2005.

Section 216 Pen Register and Trap and Trace Statute

The pen register and trap and trace statute (the "pen/trap" statute) governs the prospective collection of non-content traffic information associated with communications, such as the phone numbers dialed by a particular telephone. Section 216 updates the pen/trap statute in three important ways: (1) the amendments clarify that law enforcement may use pen/trap orders to trace communications on the Internet and other computer networks; (2) pen/trap orders issued by federal courts now have nationwide effect; and (3) law enforcement authorities must file a special report with the court whenever they use a pen/trap order to install their own monitoring device (such as the FBI's DCS1000) on computers belonging to a public provider. The following sections discuss these provisions in greater detail. (This section is not subject to the sunset provision in Section 224 of the Act).

A. Using pen/trap orders to trace communications on computer networks

Previous law: When Congress enacted the pen/trap statute in 1986, it could not anticipate the dramatic expansion in electronic communications that would occur in the following fifteen years. Thus, the statute contained certain language that appeared to apply to telephone communications and that did not unambiguously encompass communications over computer networks.3 Although numerous courts across the country have applied the pen/trap statue to communications on computer networks, no federal district or appellate court has explicitly ruled on its propriety. Moreover, certain private litigants have challenged the application of the pen/trap statute to such electronic communications based on the statute's telephone-specific language.

Amendment: Section 216 of the Act amends sections 3121, 3123, 3124, and 3127 of title 18 to clarify that the pen/trap statute applies to a broad variety of communications technologies. References to the target "line," for example, are revised to encompass a "line or other facility." Such a facility might include, for example, a cellular telephone number; a specific cellular telephone identified by its electronic serial number; an Internet user account or e-mail address; or an Internet Protocol address, port number, or similar computer network address or range of addresses. In addition, because the statute takes into account a wide variety of such facilities, amendments to section 3123(b)(1)(C) now allow applicants for pen/trap orders to submit a description of the communications to be traced using any of these or other identifiers.

Moreover, the amendments clarify that orders for the installation of pen register and trap and trace devices may obtain any non-content information – all "dialing, routing, addressing, and signaling information" – utilized in the processing and transmitting of wire and electronic communications. Such information includes IP addresses and port numbers, as well as the "To" and "From" information contained in an e-mail header. Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the "subject line" or the body of an e-mail. Agents and prosecutors with questions about whether a particular type of information constitutes content should contact the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

Further, because the pen register or trap and trace "device" often cannot be physically "attached" to the target facility, Section 216 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the amended statute allows the pen register or trap and trace device to be "attached or applied" to the target facility. Likewise, Section 216 revises the definitions of "pen register" and "trap and trace device" in section 3127 to include an intangible "process" (such as a software routine) which collects the same information as a physical device.

B. Nationwide effect of pen/trap orders

Previous law: Under previous law, a court could only authorize the installation of a pen/trap device "within the jurisdiction of the court." Because of deregulation in the telecommunications industry, however, a single communication may be carried by many providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to a local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a string of providers located throughout the country – each requiring a separate order.

Moreover, since, under previous law, a court could only authorize the installation of a pen/trap device within its own jurisdiction, when one provider indicated that the source of a communication was a different carrier in another district, a second order in the new district became necessary. This order had to be acquired by a supporting prosecutor in the new district from a local federal judge – neither of whom had any other interest in the case. Indeed, in one case investigators needed three separate orders to trace a hacker's communications. This duplicative process of obtaining a separate order for each link in the communications chain has delayed or — given the difficulty of real-time tracing — completely thwarted important investigations.

Amendment: Section 216 of the Act divides section 3123 of title 18 into two separate provisions. New subsection (a)(1) gives federal courts the authority to compel assistance from any provider of communication services in the United States whose assistance is appropriate to effectuate the order.

For example, a federal prosecutor may obtain an order to trace calls made to a telephone within the prosecutor's local district. The order applies not only to the local carrier serving that line, but also to other providers (such as long-distance carriers and regional carriers in other parts of the country) through whom calls are placed to the target telephone. In some circumstances, the investigators may have to serve the order on the first carrier in the chain and receive from that carrier information identifying the communication's path to convey to the next carrier in the chain. The investigator would then serve the same court order on the next carrier, including the additional relevant connection information learned from the first carrier; the second carrier would then provide the connection information in its possession for the communication. The investigator would repeat this process until the order has been served on the originating carrier who is able to identify the source of the communication.

When prosecutors apply for a pen/trap order using this procedure, they generally will not know the name of the second or subsequent providers in the chain of communication covered by the order. Thus, the application and order will not necessarily name these providers. The amendments to section 3123 therefore specify that, if a provider requests it, law enforcement must provide a "written or electronic certification" that the order applies to that provider.

The amendments in Section 216 of the Act also empower courts to authorize the installation and use of pen/trap devices in other districts. Thus, for example, if a terrorism or other criminal investigation based in Virginia uncovers a conspirator using a phone or an Internet account in New York, the Virginia court can compel communications providers in New York to assist investigators in collecting information under a Virginia pen/trap order.

Consistent with the change above, Section 216 of the Act modifies section 3123(b)(1)(C) of title 18 to eliminate the requirement that federal pen/trap orders specify their geographic limits. However, because the new law gives nationwide effect for federal pen/trap orders, an amendment to section 3127(2)(A) imposes a "nexus" requirement: the issuing court must have jurisdiction over the particular crime under investigation.

C. Reports for use of law enforcement pen/trap devices on computer networks

Section 216 of the Act also contains an additional requirement for the use of pen/trap devices in a narrow class of cases. Generally, when law enforcement serves a pen/trap order on a communication service provider that provides Internet access or other computing services to the public, the provider itself should be able to collect the needed information and provide it to law enforcement. In certain rare cases, however, the provider may be unable to carry out the court order, necessitating installation of a device (such as Etherpeek or the FBI's DCS1000) to collect the information. In these infrequent cases, the amendments in section 216 require the law enforcement agency to provide the following information to the court under seal within thirty days: (1) the identity of the officers who installed or accessed the device; (2) the date and time the device was installed, accessed, and uninstalled; (3) the configuration of the device at installation and any modifications to that configuration; and (4) the information collected by the device. 18 U.S.C. § 3123(a)(3).

Section 217 Intercepting the Communications of Computer Trespassers

Prior law: Although the wiretap statute allows computer owners to monitor the activity on their machines to protect their rights and property, until Section 217 of the Act was enacted it was unclear whether computer owners could obtain the assistance of law enforcement in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims to take the natural and reasonable steps in their own defense that would be entirely legal in the physical world. In the physical world, burglary victims may invite the police into their homes to help them catch burglars in the act of committing their crimes. The wiretap statute should not block investigators from responding to similar requests in the computer context simply because the means of committing the burglary happen to fall within the definition of a "wire or electronic communication" according to the wiretap statute. Indeed, because providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves, they commonly have no effective way to exercise their rights to protect themselves from unauthorized attackers. This anomaly in the law created, as one commentator has noted, a "bizarre result," in which a "computer hacker's undeserved statutory privacy right trumps the legitimate privacy rights of the hacker's victims." Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

Amendment: To correct this problem, the amendments in Section 217 of the Act allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems. Under new section 2511(2)(i), law enforcement may intercept the communications of a computer trespasser transmitted to, through, or from a protected computer. Before monitoring can occur, however, four requirements must be met. First, section 2511(2)(i)(I) requires that the owner or operator of the protected computer must authorize the interception of the trespasser's communications. Second, section 2511(2)(i)(II) requires that the person who intercepts the communication be lawfully engaged in an ongoing investigation. Both criminal and intelligence investigations qualify, but the authority to intercept ceases at the conclusion of the investigation.

Third, section 2511(2)(i)(III) requires that the person acting under color of law have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. Fourth, section 2511(2)(i)(IV) requires that investigators intercept only the communications sent or received by trespassers. Thus, this section would only apply where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of non-consenting users authorized to use the computer.

Finally, section 217 of the Act amends section 2510 of title 18 to create a definition of "computer trespasser." Such trespassers include any person who accesses a protected computer (as defined in section 1030 of title 18)4 without authorization. In addition, the definition explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). For example, certain Internet service providers do not allow their customers to send bulk unsolicited e-mails (or "spam"). Customers who send spam would be in violation of the provider's terms of service, but would not qualify as trespassers – both because they are authorized users and because they have an existing contractual relationship with the provider. These provisions will sunset December 31, 2005.

Section 220 Nationwide Search Warrants for E-mail

Previous law: Section 2703(a) requires the government to use a search warrant to compel a provider to disclose unopened e-mail less than six months old. Because Rule 41 of the Federal Rules of Criminal Procedure requires that the "property" to be obtained be "within the district" of the issuing court, however, some courts have declined to issue section 2703(a) warrants for e-mail located in other districts. Unfortunately, this refusal has placed an enormous administrative burden on those districts in which major ISPs are located, such as the Eastern District of Virginia and the Northern District of California, even though these districts may have no relationship with the criminal acts under investigation. In addition, requiring investigators to obtain warrants in distant jurisdictions has slowed time-sensitive investigations.

Amendment: Section 220 of the Act amends section 2703(a) of title 18 (and parallel provisions elsewhere in section 2703) to allow investigators to use section 2703(a) warrants to compel records outside of the district in which the court is located, just as they use federal grand jury subpoenas and orders under section 2703(d). This change enables courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of agents, prosecutors, and judges in the districts where major ISPs are located. This provision will sunset December 31, 2005.

Section 814 Deterrence and Prevention of Cyberterrorism

Section 814 makes a number of changes to improve 18 U.S.C. § 1030, the Computer Fraud and Abuse Act. This section increases penalties for hackers who damage protected computers (from a maximum of 10 years to a maximum of 20 years); clarifies the *mens rea* required for such offenses to make explicit that a hacker need only intend damage, not a particular *type* of damage; adds a new offense for damaging computers used for national security or criminal justice; expands the coverage of the statute to include computers in foreign countries so long as there is an effect on U.S. interstate or foreign commerce; counts state convictions as "prior offenses" for purpose of recidivist sentencing enhancements; and allows losses to several computers from a hacker's course of conduct to be aggregated for purposes of meeting the $5,000 jurisdictional threshold.

The following discussion analyzes these and other provisions in more detail.

A. Section 1030(c) - Raising the maximum penalty for hackers that damage protected computers and eliminating mandatory minimums

Previous law: Under previous law, first-time offenders who violate section 1030(a)(5) could be punished by no more than five years' imprisonment, while repeat offenders could receive up to ten years. Certain offenders, however, can cause such severe damage to protected computers that this five-year maximum did not adequately take into account the seriousness of their crimes. For example, David Smith pled guilty to violating section 1030(a)(5) for releasing the "Melissa" virus that damaged thousands of computers across the Internet. Although Smith agreed, as part of his plea, that his conduct caused over $80,000,000 worth of loss (the maximum dollar figure contained in the Sentencing Guidelines), experts estimate that the real loss was as much as ten times that amount.

In addition, previous law set a mandatory sentencing guidelines minimum of six months imprisonment for any violation of section 1030(a)(5), as well as for violations of section 1030(a)(4) (accessing a protected computer with the intent to defraud).

Amendment: Section 814 of the Act raises the maximum penalty for violations for damaging a protected computer to ten years for first offenders, and twenty years for repeat offenders. 18 U.S.C. § 1030(c)(4). Congress chose, however, to eliminate all mandatory minimum guidelines sentencing for section 1030 violations.

B. Subsection 1030(c)(2)(C) and (e)(8) - Hackers need only intend to cause damage, not a particular consequence or degree of damage

Previous law: Under previous law, in order to violate subsections (a)(5)(A), an offender had to "intentionally [cause] damage without authorization." Section 1030 defined "damage" as impairment to the integrity or availability of data, a program, a system, or information that (1) caused loss of at least $5,000; (2) modified or impairs medical treatment; (3) caused physical injury; or (4) threatened public health or safety.

The question repeatedly arose, however, whether an offender must *intend* the $5,000 loss or other special harm, or whether a violation occurs if the person only intends to damage the computer, *that in fact* ends up causing the $5,000 loss or harming the individuals. It appears that Congress never intended that the language contained in the definition of "damage" would create additional elements of proof of the actor's mental state. Moreover, in most cases, it would be almost impossible to prove this additional intent.

Amendment: Section 814 of the Act restructures the statute to make clear that an individual need only intend to damage the computer or the information on it, and not a specific dollar amount of loss or other special harm. The amendments move these jurisdictional requirements to 1030(a)(5)(B), explicitly making them elements of the offense, and define "damage" to mean "any impairment to the integrity or availability of data, a program, a system or information." 18 U.S.C. § 1030(e)(8) (emphasis supplied). Under this clarified structure, in order for the government to prove a violation of 1030(a)(5), it must show that the actor caused damage to a protected computer (with one of the listed mental states), and that the actor's conduct caused either loss exceeding $5,000, impairment of medical records, harm to a person, or threat to public safety. 18 U.S.C. § 1030(a)(5)(B).

C. Section 1030(c) - Aggregating the damage caused by a hacker's entire course of conduct

Previous law: Previous law was unclear about whether the government could aggregate the loss resulting from damage an individual caused to different protected computers in seeking to meet the jurisdictional threshold of $5,000 in loss. For example, an individual could unlawfully access five computers on a network on ten different dates — as part of a related course of conduct — but cause only $1,000 loss to each computer during each intrusion. If previous law were interpreted not to allow aggregation, then that person would not have committed a federal crime at all since he or she had not caused over $5,000 to any particular computer.

Amendment: Under the amendments in Section 814 of the Act, the government may now aggregate "loss resulting from a related course of conduct affecting one or more other protected computers" that occurs within a one year period in proving the $5,000 jurisdictional threshold for damaging a protected computer. 18 U.S.C. § 1030(a)(5)(B)(i).

D. 1030(c)(2)(C) - New offense for damaging computers used for national security and criminal justice

Previous law: Section 1030 previously had no special provision that would enhance punishment for hackers who damage computers used in furtherance of the administration of justice, national defense, or national security. Thus, federal investigators and prosecutors did not have jurisdiction over efforts to damage criminal justice and military computers where the attack did not cause over $5,000 loss (or meet one of the other special requirements). Yet these systems serve critical functions and merit felony prosecutions even where the damage is relatively slight. Indeed, attacks on computers used in the national defense that occur during periods of active military engagement are particularly serious — even if they do not cause extensive damage or disrupt the war-fighting capabilities of the military — because they divert time and attention away from the military's proper objectives. Similarly, disruption of court computer systems and data could seriously impair the integrity of the criminal justice system.

Amendment: Amendments in Section 814 of the Act create section 1030(a)(5)(B)(v) to solve this inadequacy. Under this provision, a hacker violates federal law by damaging a computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security," even if that damage does not result in provable loss over $5,000.

E. Subsection 1030(e)(2) - expanding the definition of "protected computer" to include computers in foreign countries

Previous law: Before the amendments in Section 814 of the Act, section 1030 of title 18 defined "protected computer" as a computer used by the federal government or a financial institution, or one "which is used in interstate or foreign commerce." 18 U.S.C. § 1030(e)(2). The definition did not explicitly include computers outside the United States.

Because of the interdependency and availability of global computer networks, hackers from within the United States are increasingly targeting systems located entirely outside of this country. The statute did not explicitly allow for prosecution of such hackers. In addition, individuals in foreign countries frequently route communications through the United States, even as they hack from one foreign country to another. In such cases, their hope may be that the lack of any U.S. victim would either prevent or discourage U.S. law enforcement agencies from assisting in any foreign investigation or prosecution.

Amendment: Section 814 of the Act amends the definition of "protected computer" to make clear that this term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2)(B). By clarifying the fact that a domestic offense exists, the United States can now use speedier domestic procedures to join in international hacker investigations. As these crimes often involve investigators and victims in more than one country, fostering international law enforcement cooperation is essential.

In addition, the amendment creates the option, where appropriate, of prosecuting such criminals in the United States. Since the U.S. is urging other countries to ensure that they can vindicate the interests of U.S. victims for computer crimes that originate in their nations, this provision will allow the U.S. to provide reciprocal coverage.

F. Subsection 1030(e)(10) - counting state convictions as "prior offenses"

Previous law: Under previous law, the court at sentencing could, of course, consider the offender's prior convictions for State computer crime offenses. State convictions, however, did not trigger the recidivist sentencing provisions of section 1030, which double the maximum penalties available under the statute.

Amendment: Section 814 of the Act alters the definition of "conviction" so that it includes convictions for serious computer hacking crimes under State law – i.e., State felonies where an element of the offense is "unauthorized access, or exceeding authorized access, to a computer." 18 U.S.C. § 1030(e)(10).

G. Subsection 1030(e)(11) -- Definition of "loss"

Previous law: Calculating "loss" is important where the government seeks to prove that an individual caused over $5,000 loss in order to meet the jurisdictional requirements found in 1030(a)(5)(B)(i). Yet prior to the amendments in Section 814 of the Act, section 1030 of title 18 had no definition of "loss." The only court to address the scope of the definition of loss adopted an inclusive reading of what costs the government may include. In United States v. Middleton, 231 F.3d 1207, 1210-11 (9th Cir. 2000), the court held that the definition of loss includes a wide range of harms typically suffered by the victims of computer crimes, including costs of responding to the offense, conducting a damage assessment, restoring the system and data to their condition prior to the offense, and any lost revenue or costs incurred because of interruption of service.

Amendments: Amendments in Section 814 codify the appropriately broad definition of loss adopted in Middleton. 18 U.S.C. § 1030(e)(11).

Section 815 Additional Defense to Civil Actions Relating to Preserving Records in Response to government Requests

Section 815 added to an existing defense to a cause for damages for violations of the Electronic Communications Privacy Act, Chapter 121 of Title 18. Under prior law it was a defense to such a cause of action to rely in good faith on a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization. This amendment makes clear that the "statutory authorization" defense includes good-faith reliance on a government request to preserve evidence under 18 U.S.C. § 2703(f).

Section 816 Development and Support of Cyber Security Forensic Capabilities

Section 816 requires the Attorney General to establish such regional computer forensic laboratories as he considers appropriate, and to provide support for existing computer forensic laboratories, to enable them to provide certain forensic and training capabilities. The provision also authorizes the spending of money to support those laboratories.

UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001

An Act :-

To deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001.in Congress assembled,

SECTION 1. SHORT TITLE AND TABLE OF CONTENTS.

(a) Short Title.--This Act may be cited as the ``Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of
2001''.

(b) Table of Contents.--The table of contents for this Act is as follows:

Sec. 1.	Short title and table of contents.
Sec. 2.	Construction; severability.

TITLE I--ENHANCING DOMESTIC SECURITY AGAINST TERRORISM

Sec. 101.	Counterterrorism fund.
Sec. 102.	Sense of Congress condemning discrimination against Arab and Muslim Americans.
Sec. 103.	Increased funding for the technical support center at the Federal Bureau of Investigation.
Sec. 104.	Requests for military assistance to enforce prohibition in certain emergencies.
Sec. 105.	Expansion of National Electronic Crime Task Force Initiative.
Sec. 106.	Presidential authority.

TITLE II--ENHANCED SURVEILLANCE PROCEDURES

Sec. 201.	Authority to intercept wire, oral, and electronic communications relating to terrorism.
Sec. 202.	Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses.
Sec. 203.	Authority to share criminal investigative information.
Sec. 204.	Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications.
Sec. 205.	Employment of translators by the Federal Bureau of Investigation.
Sec. 206.	Roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978.

Sec. 207. agents of	Duration of FISA surveillance of non-United States persons who are a foreign power.
Sec. 208.	Designation of judges.
Sec. 209.	Seizure of voice-mail messages pursuant to warrants.
Sec. 210.	Scope of subpoenas for records of electronic communications.
Sec. 211.	Clarification of scope.
Sec. 212.	Emergency disclosure of electronic communications to protect life and limb.
Sec. 213.	Authority for delaying notice of the execution of a warrant.
Sec. 214.	Pen register and trap and trace authority under FISA.
Sec. 215.	Access to records and other items under the Foreign Intelligence Surveillance Act.
Sec. 216.	Modification of authorities relating to use of pen registers and trap and trace devices.
Sec. 217.	Interception of computer trespasser communications.
Sec. 218.	Foreign intelligence information.
Sec. 219.	Single-jurisdiction search warrants for terrorism.
Sec. 220.	Nationwide service of search warrants for electronic evidence.
Sec. 221.	Trade sanctions.
Sec. 222.	Assistance to law enforcement agencies.
Sec. 223.	Civil liability for certain unauthorized disclosures.
Sec. 224.	Sunset.
Sec. 225.	Immunity for compliance with FISA wiretap.

TITLE III--INTERNATIONAL MONEY LAUNDERING ABATEMENT AND ANTI-TERRORIST FINANCING ACT OF 2001

Sec. 301.	Short title.
Sec. 302.	Findings and purposes.
Sec. 303.	4-year congressional review; expedited consideration.

Subtitle A--International Counter Money Laundering and Related Measures

Sec. 311.	Special measures for jurisdictions, financial institutions, or international transactions of primary money laundering concern.
Sec. 312.	Special due diligence for correspondent accounts and private banking accounts.
Sec. 313.	Prohibition on United States correspondent accounts with foreign shell banks.
Sec. 314.	Cooperative efforts to deter money laundering.
Sec. 315.	Inclusion of foreign corruption offenses as money laundering crimes.
Sec. 316.	Anti-terrorist forfeiture protection.
Sec. 317.	Long-arm jurisdiction over foreign money launderers.
Sec. 318.	Laundering money through a foreign bank.
Sec. 319.	Forfeiture of funds in United States interbank accounts.
Sec. 320.	Proceeds of foreign crimes.
Sec. 321.	Financial institutions specified in subchapter II of chapter 53 of title 31, United States code.
Sec. 322.	Corporation represented by a fugitive.
Sec. 323.	Enforcement of foreign judgments.

Sec. 324. Report and recommendation.
Sec. 325. Concentration accounts at financial institutions.
Sec. 326. Verification of identification.
Sec. 327. Consideration of anti-money laundering record.
Sec. 328. International cooperation on identification of originators of wire transfers.
Sec. 329. Criminal penalties.
Sec. 330. International cooperation in investigations of money laundering, financial crimes, and the finances of terrorist groups.

Subtitle B--Bank Secrecy Act Amendments and Related Improvements

Sec. 351. Amendments relating to reporting of suspicious activities.
Sec. 352. Anti-money laundering programs.
Sec. 353. Penalties for violations of geographic targeting orders and certain recordkeeping requirements, and lengthening effective period of geographic targeting orders.
Sec. 354. Anti-money laundering strategy.
Sec. 355. Authorization to include suspicions of illegal activity in written employment references.
Sec. 356. Reporting of suspicious activities by securities brokers and dealers; investment company study.
Sec. 357. Special report on administration of bank secrecy provisions.
Sec. 358. Bank secrecy provisions and activities of United States intelligence agencies to fight international terrorism.
Sec. 359. Reporting of suspicious activities by underground banking systems.
Sec. 360. Use of authority of United States Executive Directors.
Sec. 361. Financial crimes enforcement network.
Sec. 362. Establishment of highly secure network.
Sec. 363. Increase in civil and criminal penalties for money laundering.
Sec. 364. Uniform protection authority for Federal Reserve facilities.
Sec. 365. Reports relating to coins and currency received in nonfinancial trade or business.
Sec. 366. Efficient use of currency transaction report system.

Subtitle C--Currency Crimes and Protection

Sec. 371. Bulk cash smuggling into or out of the United States.
Sec. 372. Forfeiture in currency reporting cases.
Sec. 373. Illegal money transmitting businesses.
Sec. 374. Counterfeiting domestic currency and obligations.
Sec. 375. Counterfeiting foreign currency and obligations.
Sec. 376. Laundering the proceeds of terrorism.
Sec. 377. Extraterritorial jurisdiction.

TITLE IV--PROTECTING THE BORDER

Subtitle A--Protecting the Northern Border

Sec. 401. Ensuring adequate personnel on the northern border.
Sec. 402. Northern border personnel.

Sec. 403. Access by the Department of State and the INS to certain identifying information in the criminal history records of visa applicants and applicants for admission to the United States.

Sec. 404. Limited authority to pay overtime.

Sec. 405. Report on the integrated automated fingerprint identification system for ports of entry and overseas consular posts.

Subtitle B--Enhanced Immigration Provisions

Sec. 411. Definitions relating to terrorism.

Sec. 412. Mandatory detention of suspected terrorists; habeas corpus; judicial review.

Sec. 413. Multilateral cooperation against terrorists.

Sec. 414. Visa integrity and security.

Sec. 415. Participation of Office of Homeland Security on Entry-Exit Task Force.

Sec. 416. Foreign student monitoring program.

Sec. 417. Machine readable passports.

Sec. 418. Prevention of consulate shopping.

Subtitle C--Preservation of Immigration Benefits for Victims of Terrorism

Sec. 421. Special immigrant status.

Sec. 422. Extension of filing or reentry deadlines.

Sec. 423. Humanitarian relief for certain surviving spouses and children.

Sec. 424. ``Age-out'' protection for children.

Sec. 425. Temporary administrative relief.

Sec. 426. Evidence of death, disability, or loss of employment.

Sec. 427. No benefits to terrorists or family members of terrorists.

Sec. 428. Definitions.

TITLE V--REMOVING OBSTACLES TO INVESTIGATING TERRORISM

Sec. 501. Attorney General's authority to pay rewards to combat terrorism.

Sec. 502. Secretary of State's authority to pay rewards.

Sec. 503. DNA identification of terrorists and other violent offenders.

Sec. 504. Coordination with law enforcement.

Sec. 505. Miscellaneous national security authorities.

Sec. 506. Extension of Secret Service jurisdiction.

Sec. 507. Disclosure of educational records.

Sec. 508. Disclosure of information from NCES surveys.

TITLE VI--PROVIDING FOR VICTIMS OF TERRORISM, PUBLIC SAFETY OFFICERS, AND THEIR FAMILIES

Subtitle A--Aid to Families of Public Safety Officers

Sec. 611. Expedited payment for public safety officers involved in the prevention, investigation, rescue, or recovery efforts related to a terrorist attack.

Sec. 612. Technical correction with respect to expedited payments for heroic public safety officers.

Sec. 613. Public safety officers benefit program payment increase.

Sec. 614. Office of Justice programs.

Subtitle B--Amendments to the Victims of Crime Act of 1984

Sec. 621. Crime victims fund.

Sec. 622. Crime victim compensation.

Sec. 623. Crime victim assistance.

Sec. 624. Victims of terrorism.

TITLE VII--INCREASED INFORMATION SHARING FOR CRITICAL INFRASTRUCTURE PROTECTION

Sec. 701. Expansion of regional information sharing system to facilitate Federal-State-local law enforcement response related to terrorist attacks.

TITLE VIII--STRENGTHENING THE CRIMINAL LAWS AGAINST TERRORISM

Sec. 801. Terrorist attacks and other acts of violence against mass transportation systems.

Sec. 802. Definition of domestic terrorism.

Sec. 803. Prohibition against harboring terrorists.

Sec. 804. Jurisdiction over crimes committed at U.S. facilities abroad.

Sec. 805. Material support for terrorism.

Sec. 806. Assets of terrorist organizations.

Sec. 807. Technical clarification relating to provision of material support to terrorism.

Sec. 808. Definition of Federal crime of terrorism.

Sec. 809. No statute of limitation for certain terrorism offenses.

Sec. 810. Alternate maximum penalties for terrorism offenses.

Sec. 811. Penalties for terrorist conspiracies.

Sec. 812. Post-release supervision of terrorists.

Sec. 813. Inclusion of acts of terrorism as racketeering activity.

Sec. 814. Deterrence and prevention of cyberterrorism.

Sec. 815. Additional defense to civil actions relating to preserving records in response to Government requests.

Sec. 816. Development and support of cybersecurity forensic capabilities.

Sec. 817. Expansion of the biological weapons statute.

TITLE IX--IMPROVED INTELLIGENCE

Sec. 901. Responsibilities of Director of Central Intelligence regarding Foreign intelligence collected under Foreign Intelligence Surveillance Act of 1978.

Sec. 902. Inclusion of international terrorist activities within scope of foreign intelligence under National Security Act of 1947.

Sec. 903. Sense of Congress on the establishment and maintenance of intelligence relationships to acquire information on terrorists and terrorist organizations.

Sec. 904. Temporary authority to defer submittal to Congress of reports on intelligence and intelligence-related matters.

Sec. 905. Disclosure to Director of Central Intelligence of foreign intelligence-related information with respect to criminal investigations.

Sec. 906. Foreign terrorist asset tracking center.

Sec. 907. National Virtual Translation Center.

Sec. 908. Training of government officials regarding identification and use of foreign intelligence.

TITLE X--MISCELLANEOUS

Sec. 1001. Review of the department of justice.

Sec. 1002. Sense of congress.

Sec. 1003. Definition of ``electronic surveillance".

Sec. 1004. Venue in money laundering cases.

Sec. 1005. First responders assistance act.

Sec. 1006. Inadmissibility of aliens engaged in money laundering.

Sec. 1007. Authorization of funds for the police training in south and central asia.

Sec. 1008. Feasibility study on use of biometric identifier scanning system with access to the FBI integrated automated fingerprint identification system at overseas consular posts and points of entry to the United States.

Sec. 1009. Study of access.

Sec. 1010. Temporary authority to contract with local and State governments for performance of security functions at United States military installations.

Sec. 1011. Crimes against charitable Americans.

Sec. 1012. Limitation on issuance of hazmat licenses.

Sec. 1013. Expressing the sense of the senate concerning the provision of funding for bioterrorism preparedness and response.

Sec. 1014. Grant program for State and local domestic preparedness support.

Sec. 1015. Expansion and reauthorization of the crime identification technology act for antiterrorism grants to States and localities.

Sec. 1016. Critical infrastructures protection.

Comparative Study of Computer Misuse Act 1990 of UK

Computer Misuse Act 1990		**Analysis with respect to Indian Laws**
SEC.	**Substance**	
General	An Act to make provision for **securing computer material against unauthorised access or modification**; and for connected purposes. Be it enacted by the Queen's most Excellent Majesty, by and with the advice and consent of the Lords Spiritual and Temporal, and Commons, in this present Parliament assembled, and by the authority of the same, as follows:— *Computer misuse offences*	Objective of the UK Act are listed out. No comments are required.
1(1)	*Unauthorised access to computer material.* 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 section is same as section 3(1) of the Computer Misuse Act 1993 of Singapore and **hence the comments made there hold good.** However, it is worth mentioning that in the UK Act, the offence of mere unauthorized access has been dealt quite leniently [Refer section 1(3)] as compared to the subsequent offences which are committed after unauthorized access [Refer section 295)]. This approach, on one-hand causes deterrence for unauthorized access and on the other hand does not over-criminalize unauthorized access. **However in section 43 of the IT Act, mere unauthorized access is treated at par with more serious offences such as damage, computer contaminants etc. Hence, there appears to be justification for lesser punishment/ fine for mere unauthorized access especially when we have specific substantive offences in IT Act. It is recommended that necessary changes may be incorporated in the IT Act in this regard.**

1(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.	This section is same as section 3(3) of the Computer Misuse Act 1993 of Singapore and **hence the comments made there hold good.**
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	Punishment clause; does not need any comments, except that punishment for mere unauthorized access WITH knowledge and intent is a minor offence as per the UK Act.
2(1)	Unauthorised access with intent to commit or facilitate commission of further offences. 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**	The intent of this section ***appears*** to be similar as that of section 4 of Computer Misuse Act, 1993 of Singapore, i.e. criminalizing use of computer for being used as instruments. However, one notable exception in this section is that access has to be unauthorized, which need not be the case in all the cases (for example pyramid schemes). If the access is unauthorized, that per se is an offence in itself and this section merely stipulates higher punishment depending on the offence committed subsequent to unauthorized access. **Hence, as compared to this section, section 4 of Computer Misuse Act, 1993 of Singapore is**

2(2)	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 [1980 c. 43.] Magistrates' Courts Act 1980).	**Misuse Act, 1993 of Singapore is more suited to Indian law because of reasons mentioned in comments vis-à-vis that section.** On the contrary, if the intention of this section is to criminalize the various substantive acts AFTER unauthorized access - such as 'damage', 'downloading', 'copying', 'contamination' etc., then this section merely provides additional punishments for such acts. In the IT Act, various subsections of section 43 of IT Act except subsection (a), and section 66 of IT Act cover such acts and hence there is no need for any amendments/ changes in this regard.
2(3)	It is immaterial for the purposes of this section whether the further offence is to be committed **on the same occasion as the unauthorised access offence or on any future occasion**	This clarification is typical of the cyber world as computers can be programmed to commit an offence much after the unauthorized action.
2(4)	A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is **impossible**	Intent has been given paramount importance and as long as intent is to commit 'further offence' after unauthorized access, the person is punishable. **However it is debatable whether the provision providing for punishment even when further offence is impossible violates online-offline consistency principle. For example, if a person under a mistaken notion that a particular concoction will kill a person administers that concoction on a person even when it is impossible that the concoction will carry out the intended effect. That would be no offence, as no harmful result has occurred.**
2(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	Compared to section 1, the punishment prescribed for offence under section 2 is higher, which is natural as offence under section 2 is a substantive offence consequent to unauthorized access.

	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	
3(1)	Unauthorised modification of computer material. 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 subsection of this Act is same as section 5(1) of Computer Misuse Act, 1993 of Singapore and **hence the comments mentioned there hold good.**
3(2)	For the purposes of subsection (1)(b) above the requisite intent is an intent to cause a modification of the contents of any computer 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; or c. to impair the operation of any such program or the reliability of any such data	This subsection of this Act is same as section 7(1) of Computer Misuse Act, 1993 of Singapore and hence the comments mentioned there hold good.
3(3)	The intent need not be directed at— a. any particular computer; b. any particular program or data or a program or data of any particular kind; or c. any particular modification or a modification of any particular kind.	This subsection of this Act is same as section 5(3) of Computer Misuse Act, 1993 of Singapore and hence the comments mentioned there hold good
3(4)	For the purposes of subsection (1)(b) above the requisite knowledge is **knowledge that any modification he intends to cause is unauthorised.**	Further specifies 'knowledge'. Does not need any further comments than those already mentioned in case of Computer Misuse Act, 1993 of Singapore.
3(5)	It is immaterial for the purposes of this section whether an unauthorised 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.**	This subsection of this Act is same as section 5(4) of Computer Misuse Act, 1993 of Singapore and hence the comments mentioned there hold good

3(6)	For the purposes of the [1971 c. 48.] 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.	No comments.
3(7)	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	Punishment clause; needs no comments.
	Jurisdiction	
4(1)	**Territorial scope of offences under this Act.** Except as provided below in this section, it is **immaterial** for the purposes of any offence under section 1 or 3 above— a. whether any act or other event, proof of which is required for conviction of the offence occurred in the home country concerned; or b. whether the accused was in the home country concerned at the time of any such act or event.	Refer sections 5(2) and 5(3) for comments. The important aspects are that accused should be in the home country **when he does the act** (and not necessarily at the time of event or effect) OR the **affected computer resource should be in the home country for the invocation of jurisdiction**. These issues are dealt in section 5(2) and 5(3) of this Act. In the Indian context, the first issue is the normal rule of jurisdiction as per CrPC and the second rule is specifically dealt in section 75(2) of IT Act. **Hence no amendments are proposed in this regard.**
4(2)	Subject to subsection (3) below, in the case of such an offence, at least one significant link with domestic jurisdiction must exist in the circumstances of the case for the	Refer sections 5(2) and 5(3) for comments because significant links are specified there.

	offence to be committed.	
4(3)	There is no need for any such link to exist for the commission of an offence under section 1 above to be established in proof of an allegation to that effect in proceedings for an offence under section 2 above.	No comments as in India, once any of the sections in a case gives jurisdiction, jurisdiction is automatically gained for the whole case. Hence no amendments are required.
4(4)	Subject to section 8 below, where— a. any such link does in fact exist in the case of an offence under section 1 above; and b. commission of that offence is alleged in proceedings for an offence under section 2 above; section 2 above shall apply as if anything the accused intended to do or facilitate in any place outside the home country concerned which would be an offence to which section 2 applies if it took place in the home country concerned were the offence in question	No comments as in India, once any of the sections in a case gives jurisdiction, jurisdiction is automatically gained for the whole case. Hence if domestic jurisdiction exists for trial of 'unauthorized access' offence under section 1, the jurisdiction also exists for offence under section 2. Section 3 of IPC also empowers courts in India t try offences committed outside India, if they were offences in India. Hence no amendments are required. Moreover,
4(5)	This section is without prejudice to any jurisdiction exercisable by a court in Scotland apart from this section.	No comments.
4(6)	References in this Act to the home country concerned are references— a. in the application of this Act to England and Wales, to England and Wales; b. in the application of this Act to Scotland, to Scotland; and c. in the application of this Act to Northern Ireland, to Northern Ireland Significant links with domestic jurisdiction.	Irrelevant for this study.
5(1)	Significant links with domestic jurisdiction.	Does not need any comments.
5(2)	In relation to an offence under section 1, either of the following is a significant	The condition laid down in section 5(2)9a) is in consonance with the

	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.	established principle of jurisdiction in Indian Criminal Justice System. The condition laid down in 5(2)(ii) is the same as laid down in section 75 of IT Act. **Hence there is no need for any amendment in this regard.**
5(3)	In relation to an offence under section 3, 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 unauthorised modification; or (b) that the unauthorised modification took place in the home country concerned	The criterion for jurisdiction is essentially the same as laid down in preceding section, i.e. section 5(2). **Hence there is no need for any amendment in this regard.**
6(1)	Territorial scope of inchoate offences related to offences under this Act 1) On a charge of conspiracy to commit an offence under this Act the following questions are immaterial to the accused's guilt— a. the question where any person became a party to the conspiracy; and b. the question whether any act, omission or other event occurred in the home country concerned	Inchoate offences include offences related with 'conspiracy', 'attempt', 'abetment' etc. These offences have not been dealt in IT Act except for section 43(g) that deals with 'assistance'- which is strictly different from 'conspiracy', 'attempt' and 'abetment'. 'Criminal Conspiracy' is defined in section 120-A of IPC and is applicable to all offences for which punishment of 2 or more years is prescribed. **Hence conspiracy to commit any of the offences mentioned in section 65, 66 67 and 70 of IT Act can be dealt under section 120B of IPC. The law on criminal conspiracy is well defined in India. The issues mentioned in this subsection can be addressed as per the existing law and hence no amendments are required.**
6(2)	On a charge of attempting to commit	The offence of 'attempt' has not been

	an offence under section 3 above the following questions are immaterial to the accused's guilt— a. the question where the attempt was made; and b. the question whether it had an effect in the home country concerned.	addressed in the IT Act and section 511 of IPC will cover only those computer-related crimes that are covered under IPC and not under IT Act. Hence an amendment incorporating offence of 'attempt' needs to be incorporated in IT Act.
6(3)	On a charge of incitement to commit an offence under this Act the question where the incitement took place is immaterial to the accused's guilt	The offence of 'incitement' can be dealt under Chapter V of IPC. **The law is well established and does not need any amendment**.
6(4)	This section does not extend to Scotland	Does not need any comment.
7(1)	Territorial scope of inchoate offences **related to offences under external law corresponding to offences under this Act**. The following subsections shall be inserted after subsection (1) of section 1 of the [1977 c. 45.] Criminal Law Act 1977— (1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an agreement, this Part of this Act has effect in relation to it as it has effect in relation to an agreement falling within subsection (1) above. (1B) Subsection (1A) above **applies to an agreement if—** a. a party to it, or a party's agent, did anything in England and Wales in relation to it before its formation; or b. a party to it became a party in England and Wales (by joining it either in person or through an agent); or c. a party to it, or a party's agent, did or omitted anything in England and Wales in pursuance of it; and the agreement would fall within subsection (1) above as an agreement relating to the commission of a	This subsection in a nutshell deals with the principle of 'dual criminality' and the situation is dealt in section 3 of IPC and section 1(2) of IT Act. By virtue of these sections, any person may be tried in India, even if the offence was committed elsewhere. **Hence no amendments are required.**

	computer misuse offence but for the fact that the offence would not be an offence triable in England and Wales if committed in accordance with the parties' intentions."	
7(2)	The following subsections shall be inserted after subsection (4) of that section— (5) In the application of this Part of this Act to an agreement to which subsection (1A) above applies any reference to an offence shall be read as a reference to what would be the computer misuse offence in question but for the fact that it is not an offence triable in England and Wales. (6) In this section "computer misuse offence" means an offence under the Computer Misuse Act 1990."	This subsection in a nutshell deals with the principle of 'dual criminality' and the situation is dealt in section 3 of IPC and section 1(2) of IT Act. By virtue of these sections, any person may be tried in India, even if the offence was committed elsewhere. **Hence no amendments are required.**
7(3)	The following subsections shall be inserted after section 1(1) of the [1981 c. 47.] Criminal Attempts Act 1981— (1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this subsection applies to an act, what the person doing it had in view shall be treated as an offence to which this section applies. (1B) Subsection (1A) above applies to an act if— a. it is done in England and Wales; and b. it would fall within subsection (1) above as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in England and Wales.	This subsection in a nutshell deals with the principle of 'dual criminality' and the situation is dealt in section 3 of IPC and section 1(2) of IT Act. By virtue of these sections, any person may be tried in India, even if the offence was committed elsewhere. **Hence no amendments are required.**
7(4)	Subject to section 8 below, if any act done by a person in England and Wales would amount to the offence of incitement to commit an offence under	This subsection in a nutshell deals with the principle of 'dual criminality' and the situation is dealt in section 3 of IPC and section 1(2) of IT Act. By

	this Act but for the fact that what he had in view would not be an offence triable in England and Wales— a. what he had in view shall be treated as an offence under this Act for the purposes of any charge of incitement brought in respect of that act; and b. any such charge shall accordingly be triable in England and Wales.	virtue of these sections, any person may be tried in India, even if the offence was committed elsewhere. **Hence no amendments are required.**
8(1)	Relevance of external law A person is guilty of an offence triable by virtue of section 4(4) above **only if what he intended to do or facilitate would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place**.	This is a well-understood principle of Criminal Jurisprudence, applicable in Indian Law also. Hence needs no comments.
8(2)	A person is guilty of an offence triable by virtue of section 1(1A) of the [1977 c. 45.] Criminal Law Act 1977 only if the **pursuit of the agreed course of conduct** would at some stage involve— a. an act or omission by one or more of the parties; or b. the happening of some other event; constituting an offence under the law in force where the act, omission or other event was intended to take place.	This is a well-understood principle of Criminal Jurisprudence, applicable in Indian Law also. Hence needs no comments
8(3)	A person is guilty of an offence triable by virtue of section 1(1A) of the [1981 c. 47.] Criminal Attempts Act 1981 or by virtue of section 7(4) above only if **what he had in view** would involve the commission of an offence under the law in force where the whole or any part of it was intended to take place.	This is a well-understood principle of Criminal Jurisprudence, applicable in Indian Law also. Hence needs no comments
8(4)	Conduct punishable under the law in force in any place is an offence under that law for the purposes of this	This subsection recognizes the reality that same conduct constituting an offence may be described

	section, however it is described in that law	differently in different countries and for the purpose of 'dual criminality'; such different descriptions would be irrelevant if the underlying offence were the same. This principal is already practiced in Indian system of Criminal Jurisprudence and hence no amendments are required.
8(5)	Subject to subsection (7) below, a condition specified in any of subsections (1) to (3) above shall be taken to be satisfied unless not later than rules of court may provide **the defence serve on the prosecution a notice—** a. stating that, on the facts as alleged with respect to the relevant conduct, the condition is not in their opinion satisfied; b. showing their grounds for that opinion; and c. requiring the prosecution to show that it is satisfied.	Specific to trial procedures in UK. Not relevant to Indian system. In the Indian system, thee is no irrebuttable presumption in this regard and the defence can always seek proof for any doubtful fact.
8(6)	In subsection (5) above "the relevant conduct" means— a. where the condition in subsection (1) above is in question, what the accused intended to do or facilitate; b. where the condition in subsection (2) above is in question, the agreed course of conduct; and c. where the condition in subsection (3) above is in question, what the accused had in view.	Explanatory clause to subsection 8(5). No comments are needed.
8(7)	The court, if it thinks fit, may permit the defence to require the prosecution to show that the condition is satisfied without the prior service of a notice under subsection (5) above	Specific to trial procedures in UK. Not relevant to Indian system.
8(8)	If by virtue of subsection (7) above a court of solemn jurisdiction in Scotland permits the defence to require the prosecution to show that the condition	Specific to trial procedures in UK. Not relevant to Indian system.

	is satisfied, it shall be competent for the prosecution for that purpose to examine any witness or to put in evidence any production not included in the lists lodged by it.	
8(9)	In the Crown Court the question whether the condition is satisfied shall be decided by the judge alone	Specific to trial procedures in UK. Not relevant to Indian system.
8(10)	In the High Court of Justiciary and in the sheriff court the question whether the condition is satisfied shall be decided by the judge or, as the case may be, the sheriff alone.	Specific to trial procedures in UK. Not relevant to Indian system.
9(1)	British citizenship immaterial In any proceedings brought in England and Wales in respect of any offence to which this section applies it is immaterial to guilt whether or not the accused was a British citizen at the time of any act, omission or other event proof of which is required for conviction of the offence.	The principle laid down is in consonance with the 'equality before law' in India. Hence no changes are required.
9(2)	This section applies to the following offences— a. any offence under this Act; b. conspiracy to commit an offence under this Act; c. any attempt to commit an offence under section 3 above; and d. incitement to commit an offence under this Act.	By virtue of this subsection, the principle laid down in sub-section (i) is made applicable to all the offences and attempts, conspiracies and incitements to those offences. This is as per the prevalent practice in whole of Indian Law- IT Act, CrPC and IPC. Hence no changes are required.
	Miscellaneous and General	
10	Saving for certain law enforcement powers. Section 1(1) above has effect without prejudice to the operation— a. in England and Wales of any enactment relating to powers of inspection, search or seizure; and b. in Scotland of any enactment or rule of law relating to	This clause gives immunity to law enforcement powers of lawful search, seizure and inspection from the crime of unauthorized access. As long as an authorized law enforcement officer exercises these powers during an investigation, in India, they are lawful and hence automatically immune. Hence no changes are required.

	powers of examination, search or seizure.	
11(1)	Proceedings for offences under section 1. A magistrates' court shall have jurisdiction to try an offence under section 1 above if— a. the accused was within its commission area at the time when he did the act which caused the computer to perform the function; or b. any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in its commission area at that time.	No such provision exists in IT Act. Since the physical location of the cyber criminal and the affected computer can be at two entirely different locations, such a provision would clarify matters, both for the jurisdictional courts and for the jurisdictional police station. **Hence it is recommended that this section should be incorporated in the IT Act.**
11(2)	Subject to subsection (3) below, proceedings for an offence under section 1 above may be brought within a period of six months from the date on which evidence sufficient in the opinion of the prosecutor to warrant the proceedings came to his knowledge	Law of limitation is well defined in India and there is no need for an amendment in this regard.
11(3)	No such proceedings shall be brought by virtue of this section more than three years after the commission of the offence.	Law of limitation is well defined in India and there is no need for an amendment in this regard.
11(4)	For the purposes of this section, a certificate signed by or on behalf of the prosecutor and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.	Not relevant to Indian Criminal Justice System.
11(5)	A certificate stating that matter and purporting to be so signed shall be deemed to be so signed unless the contrary is proved.	Not relevant to Indian Criminal Justice System

11(6)	In this section "commission area" has the same meaning as in the Justices of the [1979 c. 55.] Peace Act 1979.	No comments.
11(7)	This section does not extend to Scotland.	Irrelevant.
12(1)	Conviction of an offence under section 1 in proceeding for an offence under section 2 or 3. If on the trial on indictment of a person charged with— a. an offence under section 2 above; or b. an offence under section 3 above or any attempt to commit such an offence; the jury find him not guilty of the offence charged, they may find him guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence brought before the expiry of any time limit under section 11 above applicable to such proceedings.	This section pertains to the judicial system in UK. Hence no comments are required. Moreover, in India, what is envisaged in this section is valid.
12(2)	The Crown Court shall have the same powers and duties in relation to a person who is by virtue of this section convicted before it of an offence under section 1 above as a magistrates' court would have on convicting him of the offence	Irrelevant.
12(3)	This section is without prejudice to section 6(3) of the [1967 c. 58.] Criminal Law Act 1967 (conviction of alternative indictable offence on trial on indictment	No comments.
12(4)	This section does not extend to Scotland	Irrelevant.
13(1)	Proceedings in Scotland. A sheriff shall have jurisdiction in	This section is wrt to jurisdiction and similar to provisions of section 75 of IT Act. **Hence changes in IT Act are**

	respect of an offence under section 1 or 2 above if— a. the accused was in the sheriffdom at the time when he did the act which caused the computer to perform the function; or b. 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 sheriffdom at that time.	**proposed.**
13(2)	A sheriff shall have jurisdiction in respect of an offence under section 3 above if— a. the accused was in the sheriffdom at the time when he did the act which caused the unauthorised modification; or b. the unauthorised modification took place in the sheriffdom.	This section is wrt to jurisdiction and similar to provisions of section 75 of IT Act. **Hence changes in IT Act are proposed.**
13(3)	Subject to subsection (4) below, summary proceedings for an offence under section 1, 2 or 3 above may be commenced within a period of six months from the date on which evidence sufficient in the opinion of the procurator fiscal to warrant proceedings came to his knowledge.	It is specific to Criminal Justice System of Scotland. Needs no comments.
13(4)	No such proceedings shall be commenced by virtue of this section more than three years after the commission of the offence	Law of limitation is well defined in India and there is no need for an amendment in this regard
13(5)	For the purposes of this section, a certificate signed by or on behalf of the procurator fiscal and stating the date on which evidence sufficient in his opinion to warrant the proceedings came to his knowledge shall be conclusive evidence of that fact.	The procedure is specific to Criminal Justice System of Scotland. Needs no comments.
13(6)	A certificate stating that matter and	The procedure is specific to Criminal

	purporting to be so signed shall be deemed to be so signed unless the contrary is proved.	Justice System of Scotland. Needs no comments.
13(7)	Subsection (3) of section 331 of the [1975 c. 21.] Criminal Procedure (Scotland) Act 1975 (date of commencement of proceedings) shall apply for the purposes of this section as it applies for the purposes of that section.	No comments
13(8)	In proceedings in which a person is charged with an offence under section 2 or 3 above and is found not guilty or is acquitted of that charge, he may be found guilty of an offence under section 1 above if on the facts shown he could have been found guilty of that offence in proceedings for that offence commenced before the expiry of any time limit under this section applicable to such proceedings.	Such a practice is prevalent in the existing trial procedures in India and no changes are proposed in this regard in the IT Act.
13(9)	Subsection (8) above shall apply whether or not an offence under section 1 above has been libelled in the complaint or indictment.	Irrelevant
13(10)	A person found guilty of an offence under section 1 above by virtue of subsection (8) above shall be liable, in respect of that offence, only to the penalties set out in section 1.	This is as per the prevalent practice in Indian Law and no changes are proposed in this regard.
13(11)	This section extends to Scotland only.	Irrelevant
14(1)	Search warrants for offences under section 1. Where a circuit judge is satisfied by information on oath given by a constable that there are reasonable grounds for believing— a. that an offence under section 1 above has been or is about to be committed in any premises; and b. that evidence that such an offence has been or is about	The Power of an investigating Officer to conduct a search with or without a warrant is well laid down in CrPC. These powers are sufficient and do not need any other amendment except that power for investigation and search should not be limited to officers of the rank of DySP and above but should be vested in any police officer whosoever is authorized by a Superintendent of Police.

	to be committed is in those premises; he may issue a warrant authorising a constable to enter and search the premises, using such reasonable force as is necessary.	
14(2)	The power conferred by subsection (1) above does not extend to authorising a search for material of the kinds mentioned in section 9(2) of the [1984 c. 60.] Police and Criminal Evidence Act 1984 (privileged, excluded and special procedure material).	Irrelevant. Refer comments for subsection 14(1).
14(3)	A warrant under this section— a. may authorise persons to accompany any constable executing the warrant; and b. remains in force for twenty-eight days from the date of its issue.	Irrelevant. Refer comments for subsection 14(1).
14(4)	In executing a warrant issued under this section a constable may seize an article if he reasonably believes that it is evidence that an offence under section 1 above has been or is about to be committed.	Irrelevant. Refer comments for subsection 14(1).
14(5)	In this section "premises" includes land, buildings, movable structures, vehicles, vessels, aircraft and hovercraft.	Irrelevant. Refer comments for subsection 14(1).
14(6)	This section does not extend to Scotland.	Irrelevant.
15	Extradition where Schedule 1 to the Extradition Act 1989 applies. The offences to which an Order in Council under section 2 of the [1870 c. 52.] Extradition Act 1870 can apply shall include— a. offences under section 2 or 3 above; b. any conspiracy to commit such an offence; and c. any attempt to commit an	This section applies to extradition and specifies extraditable offences. Hence it is irrelevant for the present study.

offence under section 3 above.

16(1) Application to Northern Ireland

The following provisions of this section have effect for applying this Act in relation to Northern Ireland with the modifications there mentioned

This section is incorporated to specify various references/ changes/ clarifications etc. for the applicability of this statute to Northern Ireland. Hence whole of section 16 is irrelevant for the present study.

16(2) In section 2(2)(b)—

a. the reference to England and Wales shall be read as a reference to Northern Ireland; and
b. the reference to section 33 of the [1980 c. 43.] Magistrates' Courts Act 1980 shall be read as a reference to Article 46(4) of the [S.I. 1981/1675 (N.I.26).] Magistrates' Courts (Northern Ireland) Order 1981

16(3) The reference in section 3(6) to the [1971 c. 48.] Criminal Damage Act 1971 shall be read as a reference to the [S.I. 1977/426 (N.I.4).] Criminal Damage (Northern Ireland) Order 1977.

16(4) Subsections (5) to (7) below apply in substitution for subsections (1) to (3) of section 7; and any reference in subsection (4) of that section to England and Wales shall be read as a reference to Northern Ireland.

16(5) The following paragraphs shall be inserted after paragraph (1) of Article 9 of the [S.I. 1983/1120 (N.I.13).] Criminal Attempts and Conspiracy (Northern Ireland) Order 1983—

(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an agreement, this Part has effect in relation to it as it has effect in relation to an agreement falling within paragraph (1).

(1B) Paragraph (1A) applies to an

agreement if—

a. a party to it, or a party's agent, did anything in Northern Ireland in relation to it before its formation;

b. a party to it became a party in Northern Ireland (by joining it either in person or through an agent); or

c. a party to it, or a party's agent, did or omitted anything in Northern Ireland in pursuance of it;

and the agreement would fall within paragraph (1) as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in Northern Ireland if committed in accordance with the parties' intentions."

16(6) The following paragraphs shall be inserted after paragraph (1) of Article 9 of the [S.I. 1983/1120 (N.I.13).] Criminal Attempts and Conspiracy (Northern Ireland) Order 1983—

(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an agreement, this Part has effect in relation to it as it has effect in relation to an agreement falling within paragraph (1).

(1B) Paragraph (1A) applies to an agreement if—

a. a party to it, or a party's agent, did anything in Northern Ireland in relation to it before its formation;

b. a party to it became a party in Northern Ireland (by joining it either in person or through an agent); or

c. a party to it, or a party's agent, did or omitted anything in Northern Ireland in pursuance of it;

and the agreement would fall within paragraph (1) as an agreement relating to the commission of a computer misuse offence but for the fact that the offence would not be an offence triable in Northern Ireland if committed in accordance with the parties' intentions.

16(7) The following paragraphs shall be inserted after Article 3(1) of that Order—

(1A) Subject to section 8 of the Computer Misuse Act 1990 (relevance of external law), if this paragraph applies to an act, what the person doing it had in view shall be treated as an offence to which this Article applies.

(1B) Paragraph (1A) above applies to an act if—

a. it is done in Northern Ireland; and
b. it would fall within paragraph (1) as more than merely preparatory to the commission of an offence under section 3 of the Computer Misuse Act 1990 but for the fact that the offence, if completed, would not be an offence triable in Northern Ireland.

16(8) In section 8—

a. the reference in subsection (2) to section 1(1A) of the [1977 c. 45.] Criminal Law Act 1977 shall be read as a reference to Article 9(1A) of that Order; and
b. the reference in subsection (3) to section 1(1A) of the [1981 c. 47.] Criminal Attempts Act 1981 shall be read as a reference to Article 3(1A) of that Order.

16(9) The references in sections 9(1) and 10 to England and Wales shall be read as references to Northern Ireland.

16(10) In section 11, for subsection (1) there shall be substituted—

(1) A magistrates' court for a county division in Northern Ireland may hear and determine a complaint charging an offence under section 1 above or conduct a preliminary investigation or preliminary inquiry into an offence under that section if—

a. the accused was in that division at the time when he did the act which caused the computer to perform the function; or
b. any computer containing any program or data to which the accused secured or intended to secure unauthorised access by doing that act was in that division at that time.

and subsection (6) shall be omitted.

16(11) The reference in section 12(3) to section 6(3) of the [1967 c. 58.] Criminal Law Act 1967 shall be read as a reference to section 6(2) of the [1967 c. 18 (N.I.).] Criminal Law Act (Northern Ireland) 1967.

16(12) In section 14—

a. the reference in subsection (1) to a circuit judge shall be read as a reference to a county court judge; and
b. the reference in subsection (2) to section 9(2) of the [1984 c. 60.] Police and Criminal Evidence Act 1984 shall be read as a reference to Article 11(2) of the [S.I. 1989/1341 (N.I. 12).] Police and Criminal Evidence (Northern Ireland) Order 1989.

17(1) Interpretation
The following provisions of this section apply for the interpretation of this Act.

Introduction to 'interpretation clause'. Needs no comments.

17(2) A person secures access to any program or data held in a computer if

Refer section 2(2) of Computer Misuse Act, 1993 of Singapore.

	by causing a computer to perform any function he— a. alters or erases the program or data; b. copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; c. uses it; or d. has it output from the computer in which it is held (whether by having it displayed or in any other manner); and references to access to a program or data (and to an intent to secure such access) shall be read accordingly	
17(3)	For the purposes of subsection (2)(c) above a person uses a program if the function he causes the computer to perform— a. causes the program to be executed; or b. is itself a function of the program.	Refer section 2(3) of Computer Misuse Act, 1993 of Singapore.
17(4)	For the purposes of subsection (2)(d) above— a. a program is output if the instructions of which it consists are output; and b. the form in which any such instructions or any other data is output (and in particular whether or not it represents a form in which, in the case of instructions, they are capable of being executed or, in the case of data, it is capable of being processed by a computer) is immaterial.	Refer section 2(4) of Computer Misuse Act, 1993 of Singapore.
17(5)	Access of any kind by any person to any program or data held in a computer is unauthorised if— a. he is not himself entitled to control access of the kind in	Refer section 2(5) of Computer Misuse Act, 1993 of Singapore.

	question to the program or data; and b. he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.	
17(6)	References to any program or data held in a computer include references to any program or data held in any removable storage medium which is for the time being in the computer; and a computer is to be regarded as containing any program or data held in any such medium.	Refer section 2(6) of Computer Misuse Act, 1993 of Singapore.
17(7)	A modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer— a. any program or data held in the computer concerned is altered or erased; or b. any program or data is added to its contents; and any act which contributes towards causing such a modification shall be regarded as causing it.	Refer section 2(7) of Computer Misuse Act, 1993 of Singapore.
17(8)	Such a modification is unauthorised if— a. the person whose act causes it is not himself entitled to determine whether the modification should be made; and b. he does not have consent to the modification from any person who is so entitled.	Refer section 2(8) of Computer Misuse Act, 1993 of Singapore.
17(9)	References to the home country concerned shall be read in accordance with section 4(6) above.	Situation in India is unambiguous and hence does not need any comments.
17(10)	References to a program include references to part of a program.	Refer section 2(9) of Computer Misuse Act 1993,Ssingapore

18(1)	Citation, commencement etc. This Act may be cited as the Computer Misuse Act 1990	Customary clause; Need no comments.
18(2)	This Act shall come into force at the end of the period of two months beginning with the day on which it is passed.	Customary clause; Need no comments.
18(3)	An offence is not committed under this Act unless every act or other event proof of which is required for conviction of the offence takes place after this Act comes into force.	Customary clause; Need no comments.

Comments on Regulation of Investigatory Powers Act of United Kingdom

INTRODUCTION

SUMMARY AND BACKGROUND

The main purpose of the Act is to ensure that the relevant investigatory powers are used in accordance with human rights. These powers are:

- the interception of communications;
- the acquisition of communications data (eg billing data);
- intrusive surveillance (on residential premises/in private vehicles);
- covert surveillance in the course of specific operations;
- the use of covert human intelligence sources (agents, informants, undercover officers);
- access to encrypted data.

For each of these powers, the Act ensures that the law clearly covers:

- the purposes for which they may be used;
- which authorities can use the powers;
- who should authorise each use of the power;
- the use that can be made of the material gained;
- independent judicial oversight;
- a means of redress for the individual.

Not all of these matters are dealt with in this Act. The Act supplements the provisions of Intelligence Services Act 1994, the Police Act 1997 and the Human Rights Act 1998.

OVERVIEW

The Act is in five parts.

Interception of Communications and the Acquisition and Disclosure of Communications Data

This Act repeals the 1985 Act and provides for a new regime for the interception of communications incorporating the changes proposed in the consultation paper. These changes go beyond what is strictly required for human rights purposes and provide also for the changed nature of the communications industry since 1985.

9. The provisions also implement Article 5 of Council Directive 97/66 of 15 December 1997, known as the "Telecommunications Data Protection Directive", which requires member states to safeguard the confidentiality of communications.

Surveillance and Covert Human Intelligence Sources

This Part provides a statutory basis for the authorisation and use by the security and intelligence agencies, law enforcement and other public authorities of covert surveillance, agents, informants and undercover officers. It will regulate the use of these techniques and safeguard the public from unnecessary invasions of their privacy.

Investigation of Electronic Data Protected by Encryption etc

This Part contains provisions to maintain the effectiveness of existing law enforcement powers in the face of increasing criminal use of encryption. Specifically, it introduces a power to require disclosure of protected (encrypted) data. Similar provision is there in the IT Act 2000.

Scrutiny of Investigatory Powers and Codes of Practice

This Part ensures that there will be independent judicial oversight of powers where necessary. It also establishes a Tribunal as a means of redress for those who wish to complain about the use of the powers. Finally, it provides for the Secretary of State to issue Codes of Practice covering the use of the powers covered by the Act.

Miscellaneous and Supplemental

This Part makes minor amendments to Wireless Telegraphy Act 1949, Part III of the Police Act 1997 in the light of operational experience and extends those provisions to the Ministry of Defence Police, the British Transport Police and the Service Police.

Both the Police Act 1997 and the Intelligence Services Act 1994 are amended to ensure authority is given for interference with property or wireless telegraphy only where it is proportionate to do so.

A brief of the relevant sections for investigation of Computer Related Crimes is as follows

COMMENTARY ON SECTIONS

Section 1: Unlawful and authorised interception

This Section creates the offences of unlawful interception and a separate civil liability for unlawful interception, explains the locations and circumstances in which each is applicable, and the circumstances in which interception is lawful.

Subsection (1) sets out the circumstances in which interception of a communication being transmitted by a public postal service or public telecommunication system is a criminal offence. The offence is similar to that created by Section 1 of the Interception of Communications Act 1985, which this Act repeals.

Subsection (2) sets out the circumstances in which interception of a communication being transmitted by a private telecommunication system is an offence. The 1985 Act contained no equivalent of this offence. There is an exclusion for the circumstances set out in subsection (6), to which this subsection refers. However, interceptions in those circumstances give rise to a civil liability.

Subsection (3) creates civil liability for unlawful interception on a private telecommunications network, the locations at which the liability applies and the persons who may bring an action under this subsection, namely the sender, recipient or intended recipient.

> *There is an exception for conduct with "lawful authority", as to which see subsection (5). Particularly relevant to this liability are the regulations that may be made under Section 4(2). For territorial limitation, see section 2(4).*

Subsection (4) applies to international agreements on mutual assistance in connection with the interception of communications which are designated under this subsection by an order made by the Secretary of State. In respect of agreements designated by this order, this subsection requires the Secretary of State to ensure that no request for mutual assistance to intercept communications, or in connection with interception, is made unless it has lawful authority.

Subsection (5) explains the circumstances in which interception of communications is lawful, and where the offences and the liability created in subsections (1), (2) and (3) do not therefore apply. These are where the interception is not authorised by an interception warrant yet falls into one of the exceptions described in Sections 3 or 4

Subsection (6) explains the circumstances in which interception falls outside the scope of the criminal offence introduced by subsection (2). This conduct attracts civil liability by virtue of subsection (3). Essentially, subsection (6) allows a person with a right to control a private telecommunication network to intercept on their own network without committing an offence. Examples of this type of activity are an individual using a second handset in a house to monitor a telephone call, and a large company in the financial sector routinely recording calls from the public in order to retain a record of transactions. Each of those cases may or may not give rise to civil liability, depending on the application of sections 3 and 4.

Subsection (7) specifies the maximum penalties for the offences created by this section. The statutory maximum referred to in paragraph (b) is currently £5000. There is no upper limit to a fine on conviction in the Crown Court.

Section 2: Meaning and location of "interception" etc

This Section sets out the definitions of telecommunications and postal services and systems relevant to the Act, and assists in the interpretation of interception and other related matters.

> *"Private telecommunication system" is defined as any telecommunication system which is not a public telecommunication system; but is attached to such a system. This means that an office network, linked to a public telecommunication system by a private exchange, is to be treated as a private system. Interception of such a system other than by the system controller or with his consent is a criminal offence. An entirely self-standing system, on the other hand, such as a secure office intranet, does not fall within the definition.*

Subsection (2) explains what constitutes the interception of a communication in the course of its transmission by means of a telecommunication system. This is relevant to the criminal offence and the civil liability in Section 1; and to the issuing of a warrant by the Secretary of State which authorises or requires interception in Section 5.

Subsection (4) explains how the territorial limitation works in Section 1(1), (2) and (3), each of which extends only to interception "at any place in the United Kingdom".

Subsection (5) excludes from the definition of interception in subsection (2) any conduct which relates only to the traffic data comprised in or attached to a communication (expanded in subsection (9)), or which relates only to so much of the content of the communication as is necessary in order to identify this traffic data.

Subsection (7) expands the phrase "while being transmitted", which is used in the tailpiece of subsection (2). The times when a communication is taken to be in the course of its transmission include any time when it is stored on the system for the intended recipient to collect or access. This means that an interception takes place, for example, where an electronic mail message stored on a web-based service provider is accessed so that its contents are made available to someone other than the sender or intended recipient, or where a pager message waiting to be collected is accessed in that way. However, if a stored communication is accessed in this way, that conduct may be lawful by virtue of Section 1(5)(c).

Subsection (9) sets out the meaning of "traffic data". It covers, for example, subscriber information under paragraph (a), and routing information under paragraph (b). Paragraph (c), which must be read with subsection (10) (which operates on subsection (5)), addresses what is commonly referred to as "dial through fraud". It covers, for example, data entered by a user seeking to arrange for a telephone call to be accepted and routed by a telecommunication system. Finally, paragraph (d) catches the data which is found at the beginning of each packet in a packet switched network which indicates which communications data attaches to which communication. The tailpiece to the definition puts beyond doubt that in relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic data may identify a server but not a website or page.

The tailpiece to the definition puts beyond doubt that in relation to internet communications, traffic data stops at the apparatus within which files or programs are stored, so the traffic may identify a server but not a website or page.

Section 3: Lawful interception without an interception warrant

This Section authorises certain kinds of interception without the need for a warrant under Section 5, namely where one or more parties to a communication have consented to the interception, conduct is in relation to the provision or operation of services, or conduct takes place with the authority of a person designated for the purposes of the Wireless Telegraphy Act 1949.

Subsection (1) authorises interception where there are reasonable grounds for believing that both the sender and the intended recipient of a communication have consented to its interception.

Subsection (2) authorises interception where:

- either the sender or intended recipient of a communication has consented to its interception; and
- the interception has been authorised under Part II (see Section 48(4)).

This situation might arise where a kidnapper is telephoning relatives of a hostage, and the police wish to record the call in order to identify or trace the kidnapper. The operation will be authorised as surveillance, rather than by means of an interception warrant.

Subsection (3) authorises interception where it takes place for the purposes of providing or operating a postal or telecommunications service, or where any enactment relating to the use of a service is to be enforced. This might occur, for example, where the postal provider needs to open a postal item to determine the address of the sender because the recipient's address is unknown.

Section 4: Power to provide for lawful interception

This Section lists the cases where a power may be exercised to provide for lawful interception without the need for a warrant under Section 5: under an international mutual assistance agreement; under regulations made by the Secretary of State to permit certain kinds of interception in the course of lawful business practice; under prison rules; in hospital premises where high security psychiatric services are provided; and in state hospitals in Scotland.

Subsection (1) enables the Secretary of State to make regulations specifying the conditions under which communication service providers may be authorised to use telecommunications systems located in the United Kingdom to intercept the communications of subjects on the territory of another country in accordance with the law of that country.

Subsection (2) makes provision for the Secretary of State to make regulations describing the kinds of interception which it is lawful to carry out in the course of the carrying on of a business. Article 5 of Directive 97/66/EC (the Telecommunications Data Protection and Privacy Directive) exempts from its prohibition on interception.

> *"Any legally authorised recording of communications in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication".*

Section 5: Interception with a warrant

This section allows for interception to be carried out when an interception warrant has been issued by the Secretary of State and sets out the grounds on which a warrant may be issued.

Subsection (1)(a) authorises the interception of communications sent by means of a postal service or telecommunication system.

Subsection (1)(b) allows the Secretary of State to issue an interception warrant for the purpose of making a request for assistance under an international mutual assistance agreement designated under Section 1(4).

Subsection (1)(c) allows the Secretary of State to issue an interception warrant for the purpose of complying with a request for assistance under an international mutual assistance agreement designated under Section 1(4).

Subsection (1)(d) allows for the disclosure of intercepted material and related communications data in a manner described by the warrant.

Subsection (2) requires that the Secretary of State may not issue an interception warrant unless he is satisfied that the warrant is necessary on grounds set out in subsection (3).

Subsection (3) sets out the grounds on which the Secretary of State may issue warrants. He may not do so unless he considers that the warrant is necessary on one of those grounds. It would not therefore be sufficient for him to consider that a warrant might be useful in supplementing other material, or that the information that it could produce could be interesting.

Subsection (6)(b) allows for related communications data to be obtained during the course of interception. For example, this could cover the actions of a provider of communications services in effecting the requirements of a warrant where the intercepted material comprises both communications and related communications data.

Section 6: Application for issue of interception warrants

65. Section 6 describes the persons who may apply for warrants.

Section 7: Issue of warrants

Section 7 describes the persons who may sign interception warrants and the circumstances in which they may do so.

The combined effect of *subsections (1) and (2)* is that the warrant must be signed by the Secretary of State unless the case is either urgent or the purpose is to comply with a request for mutual assistance where the subject of the interception or the premises and the competent authority making the request are outside the United Kingdom.

In urgent cases a warrant may be signed by a senior official. The procedure in urgent cases has three elements:

- the senior official who signs the warrant must be expressly authorised by the Secretary of State to do so (under subsection (2(a)));
- that express authorisation must be in relation to that particular warrant and
- under *subsection (4)(a)* the official who signs the warrant must endorse on it a statement that he has been expressly authorised by the Secretary of State to sign that particular warrant.

Section 8: Contents of warrant

Section 9: Duration, cancellation and renewal of warrants.

Section 10: Modification of warrants and certificates

Section 11: Implementation of warrants

Section 12: Maintenance of interception capability

Section 13: Technical Advisory Board

Section 14: Grants for interception costs

This Section requires the Secretary of State to ensure that there are arrangements to secure that communications service providers receive such a contribution as is fair in each particular case to the costs of providing an intercept capability or in the provision of assistance in respect of individual warrants.

Section 15: General safeguards

123. This Section has the effect of restricting the use of intercepted material to the minimum necessary for the authorised purposes.

Subsection (1) imposes a duty upon the Secretary of State to ensure that safeguard arrangements are in place to ensure the requirements are complied with.

Subsection (2) requires that the distribution and disclosure of intercepted material and related communications data are kept to a minimum.

Subsection (3) requires that all copies of any intercepted material and related communications data must be destroyed as soon it is no longer necessary to retain it for any of the authorised purposes.

Section 16: Extra safeguards in the case of certificated warrants

Section 17: Exclusion of matters from legal proceedings

Section 17, subject to certain exceptions, prohibits evidence, questioning or assertion in (or for the purposes of, or in connection with) legal proceedings likely to reveal the existence or absence of a warrant.

Subsection (1) imposes the basic prohibition. It does this directly, by stating that the contents of intercepted material and associated communications data may not be disclosed, and indirectly by prohibiting the disclosure of any suggestion that actions under subsection (2) have occurred.

Subsection (2) describes the actions which may not be disclosed, including actions by persons named in subsection (3) which would constitute offences under this Act or section 1 of the 1985 Act.

Section 18: Exceptions to section 17

Section 19: Offence for unauthorised disclosures

This section places a requirement upon specified groups of persons to keep secret all matters relating to warranted interception.

Subsection (4) creates the offence of unlawful disclosure and specifies the maximum penalties which a person who is found guilty of the criminal offence of unlawful disclosure may be sentenced to; if he is found guilty in a Magistrates' Court he may be imprisoned for a period up to six months or fined up to the statutory maximum (currently £5000) or both; in a Crown Court he may be imprisoned for a period up to five years, or may be fined (no upper limit), or both.

Subsection (5) gives a defence where a person could not reasonably have been expected to take steps to prevent the unlawful disclosure.

Subsections (6) and (7) give further defences to the offence of unlawful disclosure and addresses the question of a person consulting their legal adviser about requirements placed upon them under this Act, and disclosures which their legal adviser may be required to make as a result of such consultation.

Section 20

Section 20 interprets terms used in this Chapter.

CHAPTER II

This Chapter provides a legislative framework to cover the requisition, provision and handling of communications data. It explains the duties and responsibilities placed upon each party involved in these processes and creates a system of safeguards, reflecting the requirements of Article 8 of the European Convention on Human Rights.

Section 21: Lawful acquisition and disclosure of communications data

Section 22: Obtaining and disclosing communications data.

Section 23: Form and duration of authorisations and notices

Section 24: Arrangements for payments

Section 25: Interpretation of Chapter II

PART II: SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

Introductory

This Part of the Act creates a system of authorisations for various types of surveillance and the conduct and use of covert human intelligence sources. In common with other Parts of the Act, the provisions themselves do not impose a requirement on public authorities to seek or obtain an authorisation where, under the Act, one is available. Nevertheless, the consequences of not obtaining an authorisation under this Part may be, where there is an interference by a public authority with Article 8 rights and there is no other source of authority, that the action is unlawful by virtue of section 6 of the Human Rights Act 1998.

Section 26: Conduct to which Part II applies

This section describes and defines the conduct that can be authorised under this Part of the Act. Three types of activity are covered: "directed surveillance", "intrusive surveillance" and the conduct and use of covert human intelligence sources.
182. "Directed surveillance" is covert surveillance that is undertaken in relation to a specific investigation or a specific operation which is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance..
"Intrusive surveillance" is defined in *subsections (3)* to *(5)* as covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle.

Authorisation of surveillance and human intelligence sources
Section 27: Lawful surveillance etc
Section 28, 29 and 30: Authorisation of directed surveillance; Authorisation of covert human intelligence sources; and Persons entitled to grant authorisations under sections 28 and 29

Section 28 and 29 provide that authorisations cannot be granted unless specific criteria are satisfied, namely, that the person granting the authorisation believes that:

- the authorisation is necessary on specific grounds; and
- the authorised activity is proportionate to what is sought to be achieved by it.

The specific grounds are that the authorisation is necessary:

- in the interests of national security;
- for the purpose of preventing or detecting crime or preventing disorder;
- in the interests of the economic well-being of the UK;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
- for other purposes which may be specified by order of the Secretary of State.

In addition, there are two further criteria in relation to covert human intelligence sources: namely that specific arrangements exist to ensure that, amongst other things, the source is independently managed and supervised, that records are kept of the use made of the source, that the source's identity is protected from those who do not need to know it, and that arrangements also exist to satisfy such other requirements as may be imposed by order made by the Secretary of State.

Section 31: Orders under section 30 for Northern Ireland

.

INTRUSIVE SURVEILLANCE
Section 32: Authorisation of intrusive surveillance

This section deals with authorisations for intrusive surveillance.
Again, intrusive surveillance authorisations cannot be granted unless specific criteria are satisfied, namely that, the Secretary of State or senior authorising officer believes that:

- the authorisation is necessary on specific grounds; and
- the authorised activity is proportionate to what is sought to be achieved by it.

An additional factor which must be taken into account when considering whether the requirements are satisfied, is whether the information which it is thought necessary to obtain by the authorised conduct could reasonably be obtained by other means.
The specific grounds in this case are that it is necessary:

- in the interests of national security;

- for the purpose of preventing or detecting serious crime; or
- in the interests of the economic well-being of the United Kingdom.

Police and customs authorisations

Sections 33 to 40 only apply to intrusive surveillance authorisations for investigations carried out by the police,

Section 33: Rules for grant of authorisations

In the case of a police force, NCIS and the National Crime Squad, *subsection (3)* restricts an authorisation for intrusive surveillance involving residential premises to being granted only where the premises are within the area of operation of that force, Service or Squad. The areas of operations are set out in *subsection (6)*. For the three service police forces, this is defined in *subsection (7),* in terms of the persons who are subject to "service discipline".

Section 34: Grant of authorisations for intrusive surveillance in the senior officer's absence

Section 35:Notification of authorisations for intrusive surveillance

Section 36: Approval required for authorisations for intrusive surveillance to take effect

Section 37: Quashing of police and customs authorisations for intrusive surveillance etc

Section 38: Appeals against decisions by Surveillance Commissioners

Section 39: Appeals to the Chief Surveillance Commissioner: supplementary

OTHER AUTHORISATIONS

. Sections 41 and 42 also relate to intrusive surveillance authorisations, but deal with those granted by the Secretary of State.

Section 41: Secretary of State authorisations

Section 42: Intelligence services authorisations

. Where the Secretary of State grants an authorisation to one of the intelligence services under this Part (which will be for intrusive surveillance, or intrusive surveillance combined with directed surveillance), the authorisation will take the form of a warrant.

Grant, renewal and duration of authorisations

Section 43: General rules about grant, renewal and duration

Section 44: Special rules for intelligence services authorisations

Section 45: Cancellation of authorisations

Section 46: Restrictions on authorisations extending to Scotland

Supplemental provision for Part II

Section 47: Power to extend or modify authorisation provisions

Section 48: Interpretation of Part II

PART III: INVESTIGATION OF ELECTRONIC DATA PROTECTED BY ENCRYPTION ETC

Section 49: Notices requiring disclosure

This section introduces a power to enable properly authorised persons (such as members of the law enforcement, security and intelligence agencies) to serve notices on individuals or bodies requiring the disclosure of protected (e.g. encrypted) information which they lawfully hold, or are likely to, in an intelligible form.

Subsection (1) limits the information to which this power to serve notices applies. It does so by defining the various means by which the protected information in question has been, or is likely to be, lawfully obtained. By way of illustration, this could be material:

- seized under a judicial warrant (e.g. under the Police and Criminal Evidence Act 1984 (PACE));
- intercepted under a warrant personally authorised by the Secretary of State under Chapter I of Part I of this Act;

- lawfully obtained under an authorisation given under Chapter II of Part I or Part II of this Act;
- lawfully obtained by an agency under their statutory functions but not under a warrant (e.g. under the Customs and Excise Management Act 1979); or
- which has lawfully come into the possession of an agency but not by use of statutory functions (e.g. material which has been voluntarily handed over).

Subsection (2) states that persons with the "appropriate permission" may serve a notice imposing a disclosure requirement in respect of the protected information in question if there are reasonable grounds for believing:

- that the key to the relevant protected information is in the possession of the person on whom the notice is being served;
- that serving a notice imposing a disclosure requirement is necessary for the reasons set out in subsection (3), or necessary for securing the effective exercise or proper performance of any statutory power or duty of a public authority;
- that imposing a disclosure requirement is proportionate to what is sought to be achieved by doing so; and
- that an intelligible version of the relevant protected information cannot be obtained by any other reasonable means.
  key is defined in section 56(1)
  possession of a key is defined in section 56(2)

Section 50: Effect of notice imposing disclosure requirement

Section 51: Cases in which key required

This section sets out the extra tests to be fulfilled if a key is required to be disclosed rather than the disclosure of protected information in an intelligible form.

Subsection (1) states that a notice may not contain a statement that it can be complied with only by disclosing a key unless a direction to this effect has been given by the person giving permission for the notice to be served.

Section 52: Arrangements for payments for disclosure

Section 53: Failure to comply with a notice

This section creates an offence of failing to comply with the terms of a notice served under section 49.

Subsection (1) states that a person served with a notice is guilty of an offence if he knowingly fails to comply with the disclosure requirement contained in that notice.

Subsection (5) specifies the maximum sentence for the offence of failing to comply with a notice. As regards financial penalties, there is no upper limit to fines set in the Crown Court (on conviction on indictment). In a Magistrates Court (on summary conviction) the maximum fine is £5,000.

Section 54: Tipping-off

This section creates an offence where the recipient of a notice (but only one which explicitly contains a secrecy requirement), or a person that becomes aware of it, tips off another that a notice has been served, or reveals its contents. This is designed to preserve, where necessary, the covert nature of an investigation by, for example, a law enforcement agency. It outlines various statutory defences.

Section 55: General duties of specified authorities

Section 56: Interpretation of Part III

This section provides for the interpretation of various terms used in Part III of the Act.

PART IV: SCRUTINY ETC OF INVESTIGATORY POWERS AND OF THE FUNCTIONS OF THE INTELLIGENCE SERVICES

Commissioners

Section 57: Interception of Communications Commissioner

This Section provides for the appointment of an Interception of Communications Commissioner to replace the Commissioner appointed under the Interception of Communications Act 1985.

Section 58: Cooperation with and reports by s. 57 Commissioner

Section 59: Intelligence Services Commissioner

Section 61: Investigatory powers Commissioner for Northern Ireland

Section 62: Additional functions of Chief Surveillance Commissioner

Section 63: Assistant Surveillance Commissioners

This section allows for the appointment of Assistant Surveillance Commissioners to help the Chief Surveillance Commissioner fulfil his duties.

Section 64: Delegation of Commissioners' functions

This Section allows Commissioners to delegate statutory powers or duties to members of staff.

Section 65: The Tribunal

This Section establishes a Tribunal, sets out its jurisdiction and gives effect to Schedule 3, which provides for its constitution and functioning.

Section 66: Orders allocating proceedings to the Tribunal

This Section makes further provision concerning the orders that the Secretary of State may make to provide for the Tribunal to exercise jurisdiction over certain types of case. It ensures that:

- the Tribunal is given the power to remit proceedings to the court or tribunal which would have had jurisdiction but for the order;
- proceedings before the Tribunal are properly heard and considered;
- information is not disclosed where this might be damaging or prejudicial as described in subsection (2)(b).

Section 67: Exercise of the Tribunal's jurisdiction

Section 68: Tribunal procedure

Section 69: Tribunal rules

Section 70: Abolition of jurisdiction in relation to complaints

Section 71: Issue and revision of Codes of Practice

Section 72: Effect of Codes of Practice

PART V: MISCELLANEOUS AND SUPPLEMENTAL

Section 73: Conduct in relation to Wireless Telegraphy

This section amends Section 5 of the Wireless Telegraphy Act 1949 and is intended to ensure that the interception provisions of that Act comply with the Human Rights Act 1998.

Section 74: Warrants under the Intelligence Services Act 1994

This section changes the test which must be satisfied before a warrant is issued under section 5 of the Intelligence Services Act 1994. Instead of "likely to be of substantial value", the test is now that the Secretary of State must be satisfied that:

- the action is necessary for the purpose of a function of the intelligence agency;
- the action is proportionate to what it seeks to achieve;
- the action authorised by the warrant could not reasonably be achieved by other means.

345. *Subsection (3)* amends the urgent provisions so that a senior official of any department may sign an urgent warrant issued on the oral authority of the Secretary of State. Such a senior official will be a member of the Senior Civil Service or its equivalent in the Diplomatic Service.

Section 75: Authorisations under Part III of the Police Act 1997

This Section makes amendments to Part III of the Police Act 1997.

Subsections (2) and (3) amend section 93 of the Police Act to allow a police authorising officer to authorise interference with property outside his force area solely for the purpose of maintenance or retrieval of equipment.

Section 74 amends the Intelligence Services Act 1994, *subsections (4) and (5)* introduce the new tests in the Part III authorisation process. These again require that the action authorised must be necessary and proportionate to what it seeks to achieve and that the action could not reasonably be achieved by other means.

Section 76: Surveillance operations beginning in Scotland

Section 79: Criminal liability of directors etc

This Section provides for personal criminal liability on the part of certain individuals in companies and other bodies corporate.

Section 80: General saving for lawful conduct

Section 80 ensures that nothing in this Act makes any actions unlawful unless that is explicitly stated. The availability of an authorisation or a warrant does not mean that it is unlawful not to seek or obtain one. In this respect, the Act must be read with section 6 of the Human Rights Act, which makes it unlawful to act in a way which is incompatible with a Convention right.

Schedule 1: Relevant Public Authorities

Schedule 2: Persons Having the Appropriate Permission

Paragraph 2: Data obtained under warrant etc

This paragraph deals with unintelligible information which is or is likely to be obtained under a statutory power exercised in accordance with:

- a warrant issued by the Secretary of State or a person holding judicial office; or
- an authorisation under Part III of the Police Act 1997.

  Examples of legislation under which the Secretary of State may issue a warrant include Chapter I of Part I of this Act and the Intelligence Services Act 1994. Examples of legislation under which a person holding judicial office may issue a warrant include the Police and Criminal Evidence Act 1984 and the Drug Trafficking Act 1994.

Sub-paragraph (2) states that the warrant or authorisation may empower a person to serve a notice requiring disclosure if:

- the warrant or authorisation gave explicit permission for the notice to be given; or
- written permission has been given by the authority since the warrant or authorisation was issued.

Sub-paragraphs (3) to (5) describe those persons who are capable of having the appropriate permission to serve a notice in relation to material to which this paragraph applies. And *Sub-paragraphs (6) to (8)* describe those persons who may issue a warrant or authorisation in relation to such material.

The effect of this paragraph is that where, for example, protected material has been obtained under an interception warrant, the authorisation to serve a disclosure notice may be granted by the Secretary of State.

Sub-paragraph (9) excludes from this paragraph unintelligible information:

- which has been obtained under a statutory power without a warrant; but
- which has been obtained in the course of, or in connection with, an exercise of another power for which a warrant was required.

Paragraph 3: Data obtained by the intelligence services under statute but without a warrant

This paragraph deals with unintelligible information which is, or is likely to be, lawfully obtained by the intelligence services but not under a warrant issued by the Secretary of State.

Sub-paragraph (2) enables the Secretary of State to give authority for a notice to be served in such instances.

Paragraph 4: Data obtained under statute by other persons but without a warrant

This paragraph deals with unintelligible information which is or is likely to be obtained by certain agencies (other than the intelligence services) under statutory powers but not under a warrant issued by the Secretary of State or judicial authority.

Paragraph 5: Data obtained without the exercise of statutory powers

This paragraph deals with unintelligible information which is or is likely to come into the possession of an intelligence service, the police or customs and excise by any other lawful means not involving the exercise of statutory powers (e.g. material which has been voluntarily handed over).

Paragraph 6: General requirements relating to the appropriate permission

Paragraph 7: Duration of permission

Paragraph 8: Formalities for permissions granted by the Secretary of State

This paragraph states that any permissions granted by the Secretary of State in accordance with Schedule 2 may only be granted:

- if signed by him personally; or
- if signed by a member of the Senior Civil Service (or Diplomatic Service equivalent) and expressly authorised by the Secretary of State. The express authorisation must be in relation to that particular warrant (i.e. there can be no standing authorisation).

Schedule 3: The Tribunal

This Schedule provides for the constitution of the Tribunal established under Section 65.

Schedule 4

Paragraph 8: The Police Act 1997 (c.50)

This makes necessary consequential changes in the light of the amendments to Part III of the Police Act 1997. These take account of the extension of authorising powers to the Ministry of Defence Police, the British Transport Police, the Service Police, the three service police forces, the Deputy Director General of the National Crime Squad and additional designated customs officers.

389. *Sub-paragraph (10)* extends the functions of the Chief Surveillance Commissioner so that he reports annually to the Prime Minister and at any other time on any matters arising from his functions in relation to Part III of the Police Act 1997 or Part II of this Act.

390. *Sub-paragraph (11)* imposes a duty on those exercising functions under these provisions to disclose or provide the Chief Surveillance Commissioner with any documents or information he requires to enable him to carry out his functions. It also imposes a duty on every Commissioner to give the Tribunal established under section 65 of this Act all such assistance as may be required.

Supplement to RIP Act

Unlawful Interception.

1.1 It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of-

a. a public postal service; or
b. a public telecommunication system.

1.2 It shall be an offence for a person-

a. intentionally and without lawful authority, and
b. otherwise than in circumstances in which his conduct is excluded by subsection (6) from criminal liability under this subsection,

to intercept, at any place in the United Kingdom, any communication in the course of its transmission by means of a private telecommunication system.

1.3 Any interception of a communication which is carried out at any place in the United Kingdom by, or with the express or implied consent of, a person having the right to control the operation or the use of a private telecommunication system shall be actionable at the suit or instance of the sender or recipient, or intended recipient, of the communication if it is without lawful authority and is either-

a. an interception of that communication in the course of its transmission by means of that private system; or
b. an interception of that communication in the course of its transmission, by means of a public telecommunication system, to or from apparatus comprised in that private telecommunication system.

1.4 Where the United Kingdom is a party to an international agreement which-

a. relates to the provision of mutual assistance in connection with, or in the form of, the interception of communications,
b. requires the issue of a warrant, order or equivalent instrument in cases in which assistance is given, and
c. is designated for the purposes of this subsection by an order made by the Secretary of State,

it shall be the duty of the Secretary of State to secure that no request for assistance in accordance with the agreement is made on behalf of a person in the United Kingdom to the competent authorities of a country or territory outside the United Kingdom except with lawful authority.

1.5 Conduct has lawful authority for the purposes of this section if, and only if-

a. it is authorised by or under section 3 or 4;
b. it takes place in accordance with a warrant under section 5 ("an interception warrant"); or
c. it is in exercise, in relation to any stored communication, of any statutory power that is exercised (apart from this section) for the purpose of obtaining information or of taking possession of any document or other property;

and conduct (whether or not prohibited by this section) which has lawful authority for the purposes of this section by virtue of paragraph (a) or (b) shall also be taken to be lawful for all other purposes.

1.6 The circumstances in which a person makes an interception of a communication in the course of its transmission by means of a private telecommunication system are such that his conduct is excluded from criminal liability under subsection (2) if-

a. he is a person with a right to control the operation or the use of the system; or
b. he has the express or implied consent of such a person to make the interception.

1.7 A person who is guilty of an offence under subsection (1) or (2) shall be liable-

a. on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine, or to both;
b. on summary conviction, to a fine not exceeding the statutory maximum.

1.8 No proceedings for any offence which is an offence by virtue of this section shall be instituted-

a. in England and Wales, except by or with the consent of the Director of Public Prosecutions;
b. in Northern Ireland, except by or with the consent of the Director of Public Prosecutions for Northern Ireland.

Comparative study of Computer Misuse Act 1993 of Singapore

Computer Misuse Act 1993		Analysis with respect to Indian Laws
Sec.	**Substance of Section**	**Comments**
1.	This **Act** may be cited as the **Computer Misuse Act**	In India, the Offences arising out of Computer Misuse are covered in IT Act, the Indian Penal Code and the proposed Communications Convergence Bill.
2(1)	In this **Act**, unless the context otherwise requires -	
	"**Computer**" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices, but does not include -- (a) an automated typewriter or typesetter; (b) a portable hand held calculator; (c) a similar device which is non-programmable or which does not contain any data storage facility; or (d) such other device as the Minister may, by notification in the Gazette, prescribe;	Section 2(l) (i) of the IT Act defines the term 'Computer', section 2 (l)(j) defines 'Computer Network', section 2(l) (k) defines 'Computer Resource' and section 2(l)(l) defines 'Computer System'. As in the IT Act, the terms 'Computer', 'Computer System' and 'Computer Network' are mostly used together, a combined reading of all these sections covers all conceivable combinations of Information Technology. **There is no need to amend any of these definitions.**
	"**computer** output" or "output" means a statement or representation (whether in written, printed, pictorial, graphical or other form) purporting to be a statement or representation of fact -- (a) produced by a **computer**; or (b) accurately translated from a statement or representation so produced;	This term has not been defined in the IT Act. However, the term 'Electronic Record' has been defined in section 2(l) (t) and 'Information' is defined in section 2 (l)(v) of the Act. As the term 'Computer Output' is not much relevant to IT Act, **there is no need for an amendment in this regard.**
	"**computer** service" includes **computer** time, data processing and	This term is not defined in the IT Act. **However, with intangible property such as computer data acquiring the meaning of property in the cyber world, it would be appropriate to incorporate this definition also in the IT Act. This will also clarify the scope**

the storage or retrieval of data;	**of section 43 (h) of IT Act by clearly making the theft of internet time as an offence.**
"damage" means, except for the purposes of section 13, any impairment to a **computer** or the integrity or availability of data, a program or system, or information, that -- (a) causes loss aggregating at least $10,000 in value, or such other amount as the Minister may, by notification in the Gazette, prescribe except that any loss incurred or accrued more than one year after the date of the offence in question shall not be taken into account; (b) modifies or impairs, or potentially modifies or impairs, the medical examination, diagnosis, treatment or care of one or more persons; (c) causes or threatens physical injury or death to any person; or (d) threatens public health or public safety;	The term 'Damage' is defined in section 43, explanation (iv) of the IT Act. Although the ingredients of the term 'damage' are covered by both the definitions- in the Singapore as well as the IT Act, the Singapore Act has limited the definition to include either to only those instances where the loss is not trivial in monetary terms or to cases where damage is caused in areas of public health / law and order. The concept is very sound as it automatically excludes trivial 'damages' from the ambit of criminal law on one hand thereby reducing litigation and on the other hand, it encourages the users to take measures for information security. **The definition of 'damage' in the IT Act can hence be suitably amended by incorporating similar limiting clauses. Alternately, restriction can be in terms of either 'secure information' or 'protected computers'.**
"data" means representations of information or of concepts that are being prepared or have been prepared in a form suitable for use in a **computer**;	The term 'data' is defined in section 2 (I)(o) of the IT Act and is essentially the same as the instant definition. **No amendments are proposed**.
"electronic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a **computer**;	**This definition is wrt the term 'interception', which has not been defined in the IT Act.**
"function" includes logic, control,	The term is defined similarly in section 2(I)(u) of the IT Act. **No Amendment is required.**

	arithmetic, deletion, storage and retrieval and communication or telecommunication to, from or within a **computer**;	
	"intercept" , in relation to a function of a **computer**, includes listening to or recording a function of a **computer**, or acquiring the substance, meaning or purport thereof;	The term 'Interception' has not been defined in the IT Act, although it finds mention in section 69 (I) of the IT Act. **Both for the purpose of clarifying section 69 of the IT Act and also for interpreting the offences of unauthorized interception, it is recommended to include this definition in section 2 of IT Act.**
	"program or **computer** program" means data representing instructions or statements that, when executed in a **computer**, causes the **computer** to perform a function.	**The term is well understood in computer parlance and there is no need for any amendment.**
2(2)	For the purposes of this **Act**, a person secures access to any program or data held in a **computer** if by causing a **computer** to perform any function he -- (a) alters or erases the program or data; (b) copies or moves it to any storage medium other than that in which it is held or to a different location in the storage medium in which it is held; (c) uses it; or (d) causes it to be output from the **computer** in which it is held (whether by having it displayed or in any other manner), and references to access to a program or data (and to an intent to secure such access) shall be read accordingly.	The term 'access' is defined in section 2 (I) (a) of the IT Act and if read with definitions of 'Computer', 'Computer System', 'computer network', the definition in IT Act covers all possible actions that are being covered by the instant definition. Moreover, the definition in the IT Act limits itself only to actus reus and does not further specify the result of action, as is the approach in the Singapore Law. **Hence there is no need for any amendment.**
2(3)	For the purposes of subsection (2) (c), a person uses a program if the function he causes the **computer** to perform -- (a) causes the program to be executed; or (b) is itself a function of the program	No comment as this is only a clarification in the context of definition of the term 'securing access' defined in preceding paragraph. **There is no need for any amendment in the IT Act.**

2(4)	For the purposes of subsection (2) (d), the form in which any program or data is output (and in particular whether or not it represents a form in which, in the case of a program, it is capable of being executed or, in the case of data, it is capable of being processed by a **computer**) is immaterial	No comment as this is only a clarification in the context of definition of the term 'securing access' defined in preceding paragraph**. There is no need for any amendment in the IT Act.**
2(5)	For the purposes of this **Act**, access of any kind by any person to any program or data held in a **computer** is unauthorized or done without authority if -- (a) he is not himself entitled to control access of the kind in question to the program or data; and (b) he does not have consent to access by him of the kind in question to the program or data from any person who is so entitled.	This term 'unauthorized access' is not defined in the IT Act. In section 43 of the IT Act, the words used for unauthorized access are ' without the permission of owner or any other person who is in charge of a computer…'. However the approach of the IT Act leaves the question of 'exceeding authority of access' which is addressed in the Singapore Law by the words ' access of the kind in question' in section 2(5)(b). **The necessary amendment can be made in the IT Act in this regard as computer-related crimes, especially concerning fraud etc., are likely to entail situations of exceeding authority for access.**
2(6)	A reference in this **Act** to any program or data held in a **computer** includes a reference to any program or data held in any removable storage medium which is for the time being in the **computer**; and a **computer** is to be regarded as containing any program or data held in any such medium	This situation is addressed by the IT Act through wide definition of terms of 'Computer', 'Computer System', 'computer network' and their usage together. **Hence there is no need for any amendment in this regard.**
2(7)	For the purposes of this **Act**, a modification of the contents of any **computer** takes place if, by the operation of any function of the **computer** concerned or any other **computer** -- (a) any program or data held in the **computer** concerned is altered or erased; (b) any program or data is added to its contents; or (c) any **act** occurs which impairs the	The term 'modify' is not defined in the IT Act. The term has been used in section 43, Explanation (i)(a). However in the IT Act, in sections 43, 65 and 66 of IT Act, the end results listed in instant section of the Singapore Law-such as deletion, alteration, disruption of computer etc. are separately mentioned. **There is no need for any amendment in this regard.**

	normal operation of any **computer**, and any **act** which contributes towards causing such a modification shall be regarded as causing it	
2(8)	Any modification referred to in subsection (7) is unauthorized if -- (a) the person whose **act** causes it is not himself entitled to determine whether the modification should be made; and (b) he does not have consent to the modification from any person who is so entitled	This is a clarification on the lines similar to 'authorized access'. The comments wrt section 2(5) hold good for this section also.
2(9)	(9) A reference in this **Act** to a program includes a reference to part of a program	This is a trivial clarification and does not need any comment.
3(1)	Subject to subsection (2), any person who knowingly causes a **computer** to perform any function for the purpose of securing access without authority to any program or data held in any **computer** shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both	The basic offence covered here is that of 'KNOWING unauthorized access'. This offence is covered in section 43(a) of IT Act, which is a civil wrong and section 70 of IT Act (for unauthorized access to protected systems). However section 43 does not require the condition of 'knowing' to be fulfilled. **It is proposed that this requirement should be incorporated in the IT Act and section 43 should be amended accordingly.**
3(2)	If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both	Whereas subsection (i) criminalizes the mere unauthorized access, this subsection entails harsher punishment if unauthorized access causes 'damage' as defined in section 2(l) of the IT Act. This aspect is covered in section 43(d) (though without any harsher punishment), section 65 & 66 of the IT Act. **Hence no more modification of he IT Act, apart from those already mentioned, are needed in this regard.**
3(3)	For the purposes of this section, it is immaterial that the **act** in question is not directed at --	This clarification is desirable though not essential. **The Indian Law in the IT Act (sections 43, 66 and 70) as it exists,**

	(a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular **computer**	**does not require this clarification and there is no need for any amendment in this regard.**
4(1)	Any person who causes a **computer** to perform any function for the purpose of securing access to any program or data held in any **computer** with intent to commit an offence to which this section applies shall be guilty of an offence	There is no such offence in the IT Act. Generally, the offences such as fraud (cheating as per Indian Law), forgery or any other bodily harm is covered by the IPC- without any amendment if the existing law is technologically neutral, or else with minor amendments to suit cyber world, if required. In India, the IT Act has amended the IPC mainly by the inclusion of the term 'electronic documents' in 'document' related offences. Whereas this achieves the objective of making the relevant acts even when committed in cyber world as crimes under the IPC, problems are created on procedural front such as extra-territorial jurisdiction and international cooperation. The IT Act gives extra territorial jurisdiction for offences under the IT Act, by virtue of sections 1(2) and 75 of the IT Act, but such jurisdiction in terms of section of 3 & 4 of IPC is not available for IPC offences. Through the inclusion of such a section as this, IT Act can be invoked in all those IPC offences where computers are used thereby ensuring that extra-territorial jurisdiction provisions of IT Act can be used even in the IPC cases where computers are used as instruments (pyramidal investment schemes for instance) without any amendments in IPC. **Hence it is strongly recommended that this section be included in IT Act.**
4(2)	This section shall apply to an offence involving property, fraud, dishonesty or which causes bodily harm and which is punishable on conviction with imprisonment for a term of not less than 2 years	The provision of including only those offences in which punishment is more than 2 years is a sound one, as most extradition statutes also have this condition. **This provision is also recommended for inclusion in the proposed section mentioned in preceding section in the IT Act.**

4(3)	Any person guilty of an offence under this section shall be liable on conviction to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 10 years or to both	As international cooperation will generally be based on principles similar to extradition (such as 'dual criminality' and 'minimum 2 years imprisonment'), **therefore, the punishment for the proposed section should be above 2 years.**
4(4)	For the purposes of this section, it is immaterial whether -- (a) the access referred to in subsection (1) is authorised or unauthorized; (b) the offence to which this section applies is committed at the same time when the access is secured or at any other time	These provisions are clarifications of substantive offence under sections 4(1) and 4(2) of the Singapore Act and need to be incorporated in the proposed similar section in IPC. As computer will be used mostly as an instrument to commit a crime in these cases, therefore, although clarifications of this section follow as a natural corollary, **there is no harm if the clarification is also incorporated in the IT Act under the proposed section as an 'explanation'**
5(1)	Subject to subsection (2), any person who does any **act** which he knows will cause an unauthorized modification of the contents of any **computer** shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both	This section covers those acts where the perpetrator does any act with the knowledge that the act will cause an unauthorized modification of contents of any computer, whether the modification is actually caused or not, whether it is permanent or temporary or whether it is not directed at any particular program or data or any particular computer. Such an act can be easily covered under the act of introduction of a 'computer contaminant' [as defined in section 43, explanation (i)] which is a civil wrong under section 43 © of IT Act. **However, the requirement of 'knowledge' is absent in whole of section 43 and recommendation of its inclusion has already been made in earlier sections.** Sections 43(d) and section 66 of IT Act can also be used to cover such Acts wherever damage, destruction, alteration or deletion is actually caused. Hence there is no need for an amendment.
5(2)	If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both	As mentioned above, Sections 43©, 43 (d) and 66 of IT Act amply cover the acts where unauthorized damage is actually caused. **Hence no amendments are required in this regard.**

5(3)	For the purposes of this section, it is immaterial that the **act** in question is not directed at -- (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular **computer**	This clarification is desirable but not essential, as the IT Act either does away with the 'intent' and 'knowledge' altogether as in case of section 43 of IT Act or does not require any specific act on a particular program, data or computer but only requires the knowledge that the Act will cause damage to any person, as in case of section 66 of IT Act. **Hence no amendments are required in this regard.**
5(4)	For the purposes of this section, it is immaterial whether an unauthorized modification is, or is intended to be, permanent or merely temporary	The definitions of the word 'damage' [in section 43, explanation (iv) of IT Act] and of 'wrongful loss' in the section 23 of IPC do not talk of any permanency of damage or loss and hence **this clarification is not necessary in the IT Act.**
6(1)	Subject to subsection (2), any person who knowingly --	
	(a) secures access without authority to any **computer** for the purpose of obtaining, directly or indirectly, any **computer** service;	'Unauthorized access' per se is an offence under the IT Act vide section 43 (a). Hence, if the access is for the purpose of obtaining any 'computer service' i.e. 'computer time, data processing and the storage or retrieval of data', it shall also be covered under section 43(a) of the IT Act besides section 43 (b), 43 (h) or section 66 of IT Act depending upon the circumstances of the case. **Hence there is no need for any amendment in this regard.**
	(b) intercepts or causes to be intercepted without authority, directly or indirectly, any function of a **computer** by means of an electro-magnetic, acoustic, mechanical or other device; or	This section criminalizes the unauthorized act of 'interception' of a computer service. 'Unauthorized Interception' is not covered in the IT Act as such although it appears that unauthorized 'downloading' of information from 'computer, computer system or computer network' as per section 43(b) of IT Act or 'diminishing the utility of information' residing in a 'computer resource' [which includes a computer network also] as per section 66 of IT Act can be used to cover this

	(c) uses or causes to be used, directly or indirectly, the **computer** or any other device for the purpose of committing an offence under paragraph (a) or (b), shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both	offense. Moreover, section 63 (4) of the proposed Communications Convergence Bill also makes 'unauthorized Interception' a specific Offence. **Hence there is no need for any amendment in this regard.** This subsection criminalizes the use or causing the use of computer or any other device for use- directly or indirectly- for causing an offence of unauthorized access for availing computer service or interception. Section 43 (g) of IT Act can take care for abetment (i.e. causes to be used). The user himself is liable otherwise for the substantive offence itself. **Hence there is no need for any amendment in this regard.**
6(2)	If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both	This subsection ensures higher punishment in the event that 'damage' is caused in the process of offences listed in subsection (i). In IT Act, the person can also be liable u/s 43(d), 65 or 66 IT Act in case damage is caused, depending on facts and circumstances of the case. **Hence there is no need for any amendment.**
6(3)	For the purposes of this section, it is immaterial that the unauthorized access or interception is not directed at -- (a) any particular program or data; (b) a program or data of any kind; or (c) a program or data held in any particular **computer**	This clarification is same as that given in section 5(3) and comments given there hold good here also.
7(1)	Any person who, knowingly and without authority or lawful excuse --	
	(a) interferes with, or interrupts or obstructs the lawful use of, a **computer**; or (b) impedes or prevents access to, or impairs the usefulness or effectiveness of, any program or data stored in a **computer**,	This section aims to cover offences such as 'denial of service'. This section also penalizes any act that impairs the usefulness or effectiveness of any program, or data stored in a computer. Only unauthorized conduct with knowledge has been made a penal offence in the Singapore Act. Such acts can be covered under section 43(e), 43

	shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both	(f) and section 66 of IT Act. **Hence there is no need for any amendment in this regard.**
7(2)	If any damage is caused as a result of an offence under this section, a person convicted of the offence shall be liable to a fine not exceeding $50,000 or to imprisonment for a term not exceeding 7 years or to both	'Damage' is already covered in section 43 (d) of IT Act. Hence there is no need for any amendment in this regard.
8(1)	Any person who, knowingly and without authority, discloses any password, access code or any other means of gaining access to any program or data held in any **computer** shall be guilty of an offence if he did so -- (a) for any wrongful gain; (b) for any unlawful purpose; or (c) knowing that it is likely to cause wrongful loss to any person	This offence can be covered under section 43(g) of the IT Act although that section does not require any specific intent. However, this type of conduct can also be covered by 'abetment' sections under IPC and hence there is no need for any amendment in this regard.
8(2)	Any person guilty of an offence under subsection (1) shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a second or subsequent conviction, to a fine not exceeding $20,000 or to imprisonment for a term not exceeding 5 years or to both	This subsection only prescribes the punishment and hence does not need any comment.
9(1)	Where access to any protected **computer** is obtained in the course of the commission of an offence under section 3, 5, 6 or 7, the person convicted of such an offence shall, in lieu of the punishment prescribed in those sections, be liable on conviction to a fine not exceeding $100,000 or to imprisonment for a term not exceeding 20 years or to both	This section aims for enhanced punishment for unauthorized access to 'protected computers' in the course of commission of an offence dealt earlier in sections 3, 5, 6 or 7 of the IT Act. The IT Act deals with this situation by making mere unauthorized access to a protected system an offence under section 70(3) of IT Act. Thus in India, if somebody gets unauthorized access to a protected computer and also commits another

		offence after the access, he can be prosecuted for two separate offences and is thus liable for a higher quantum of punishment. **Hence there is no need for amendment in this regard**.
9(2)	For the purposes of subsection (1), a **computer** shall be treated as a "protected **computer**" if the person committing the offence knew, or ought reasonably to have known, that the **computer** or program or data is used directly in connection with or necessary for -- (a) the security, defence or international relations of **Singapore**; (b) the existence or identity of a confidential source of information relating to the enforcement of a criminal law; (c) the provision of services directly related to communications infrastructure, banking and financial services, public utilities, public transportation or public key infrastructure; or (d) the protection of public safety including systems related to essential emergency services such as police, civil defence and medical services	This subsection defines a broad category of computers which will be treated as 'protected computers' based on two criterion namely use of computer/data/program and knowledge of that use by the perpetrator. The knowledge is either presumed as per subsection(3) or assumed to have been caused through electronic display of warning. As opposed to this approach, the IT Act, as per section 70(1), leaves it to the appropriate government to declare any computer to be a protected computer. The advantage of the Indian approach is that the Govt. will ensure the compliance of the security guidelines contained in Cyber Regulations before declaring any computer as 'protected computer'. However, the Singapore approach is beneficial from the point of view of enforceability as well causing of deterrence. **Hence, it is proposed that suitable amendment should be made in the IT Act in section 70(1) to specify what are 'protected systems' on the same lines as the instant section in the Singapore Law and also incorporating the assumption of knowledge as per subsection (3) of the instant section of Singapore Act.**
9(3)	For the purposes of any prosecution under this section, it shall be presumed, until the contrary is proved, that the accused has the requisite knowledge referred to in subsection (2) if there is, in respect of the **computer**, program or data, an electronic or other warning exhibited to the accused stating that unauthorized access to that **computer**, program or data attracts an enhanced penalty under this section	**Already dealt in discussion of subsection (2) and recommended for inclusion in amendment in the IT Act.**

10(1)	Any person who abets the commission of or who attempts to commit or does any **act** preparatory to or in furtherance of the commission of any offence under this **Act** shall be guilty of that offence and shall be liable on conviction to the punishment provided for the offence	'Attempt' and 'Aiding or abetments' are already substantive offences under various sections of IPC. Attempt is covered under section 511 of IPC for attempting to commit offences under IPC and hence may not cover all offences in the IT Act (as it exists and along with proposed amendments). **Therefore, a separate section analogous to section 511 of IPC and the present section of the Convention for attempt needs to be legislated. Additionally, attempt for only Illegal Interception, Data Interference, System Interference and Section 67 of IT Act need to be criminalized as the rest of the offences are either covered in IPC or are not realistically possible to attempt with any appreciable effect without committing.** Abetment is covered in section 109 to 111 of IPC and since it is not tied to offences in IPC alone, will cover all offences under any Act. Aiding is also covered partly by section 43(g) of the IT Act. Hence no fresh section needs to be legislated in this regard.
10(2)	For an offence to be committed under this section, it is immaterial where the **act** in question took place	Attempt automatically means that act was not done. Abetment as defined in sections 107 and 108 of IPC also includes this condition. **Hence there is no need for any amendment.**
11(1)	Subject to subsection (2), the provisions of this **Act** shall have effect, in relation to any person, whatever his nationality or citizenship, outside as well as within **Singapore**	This section deals with extra-territorial jurisdiction of the Singapore Act. The same objective is achieved in the IT Act through sections 1(2) and 75 of the Act. The conditions under which the extra-terrotorial jurisdiction is invoked are also similar to the Singapore Act, i.e. the person committing the offence should be in India (which needs no statement being in accordance with normal principles of Indian Criminal Jurisprudence) **or** computer, computer system or computer
11(2)	Where an offence under this **Act** is committed by any person in any place outside **Singapore**, he may be dealt with as if the offence had been committed within **Singapore**.	

11(3)	For the purposes of this section, this **Act** shall apply if, for the offence in question -- (a) the accused was in **Singapore** at the material time; or (b) the **computer**, program or data was in **Singapore** at the material time	computer, computer system or computer network involved in the offence must e located in India. **Hence the law in IT Act is analogous to the Singapore Law and there is no need for any amendment.**
12	A District Court or a Magistrate's Court shall have jurisdiction to hear and determine all offences under this **Act** and, notwithstanding anything to the contrary in the Criminal Procedure Code (Cap. 68), shall have power to impose the full penalty or punishment in respect of any offence under this **Act**	Does not need any comment as the judicial/ administrative/ quasi-judicial/ adjudicatory set-up is well defined in the IT Act also.
13(1)	The court before which a person is convicted of any offence under this **Act** may make an order against him for the payment by him of a sum to be fixed by the court by way of compensation to any person for any damage caused to his **computer**, program or data by the offence for which the sentence is passed	This power already exists in Indian Criminal Justice System and also under the IT Act and hence does not require any amendment.
13(2)	Any claim by a person for damages sustained by reason of the offence shall be deemed to have been satisfied to the extent of any amount which has been paid to him under an order for compensation, but the order shall not prejudice any right to a civil remedy for the recovery of damages beyond the amount of compensation paid under the order.	This is also a standard practice in Indian Jurisprudence as the principle of 'Double Jeopardy' is applicable only in case of criminal liability. However, under the IT Act, the compensation/ penalty is limited to an amount of Rs. 1 crore only.
13(3)	An order of compensation under this section shall be recoverable as a civil debt.	This is a standard practice in Indian Jurisprudence and hence does not need any comment
14	Nothing in this **Act** shall prohibit a police officer, a person authorised in writing by the Commissioner of Police under section 15 (1) or any other duly authorised law enforcement officer from lawfully conducting investigations pursuant to his powers conferred	Vide section 78 of the IT Act limits the power of investigation of offences under the IT Act to police officers above the rank of DySPs only. This creates an anomalous situation because some computer-related crimes are proposed to be dealt in India under the IPC alone

	under any written law	such as 'Cheating' (pyramidal investment schemes). Such IPC Offences, even though involving computers can be investigated even by Head Constables, as there is no restriction based on rank of IO in CrPC. **Hence it is proposed that this anomaly should be removed by vesting the District Superintendent of Police to authorize police Officers to conduct Investigations in Computer-related Crimes, based on their knowledge, skills and laid down guidelines. This will also avoid the problem of having insufficient manpower for investigation of Computer-related crimes and at the same time lead to capacity building in Police Department.**
15(1)	A police officer or a person authorised in writing by the Commissioner of Police shall -- (a) be entitled at any time to -- (i) have access to and inspect and check the operation of any **computer** to which this section applies; (ii) use or cause to be used any such **computer** to search any data contained in or available to such **computer**; or (iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such **computer** into readable and comprehensible format or text for the purpose of investigating any offence under this **Act** or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section; (b) be entitled to require -- (i) the person by whom or on whose behalf, the police officer or	In India, as per CrPC, any Investigating Officer is automatically vested with power of searching of computers during an investigation. However, the IT Act places two restrictions on these powers. Firstly, only a police Officer of and above the rank of a Dy. Superintendent of Police can investigate an offence under the IT Act. The problems associated with this provision and solution thereof has already been mentioned in the preceding section. The second restriction is unique to computer technology and involves the use of encryption, passwords, hardware locks (such as dongels etc.) by the suspects. Without access to appropriate technology and obligation of providing technical assistance and disclose passwords etc. on part of owner of computer or any other person having requisite knowledge, it is impossible to conduct search of a computer. The IT Act realizes this problem, but only partially. Firstly, only decryption has been mentioned in section 69 , and no mention has been made of passwords, hardware locks etc. Secondly, the power has been vested in only the CCA, which is impractical given the nature of technology involved and size of the country. In the Singapore Act, these

	investigation officer has reasonable cause to suspect, any **computer** to which this section applies is or has been used; or (ii) any person having charge of, or otherwise concerned with the operation of, such **computer**, to provide him with such reasonable technical and other assistance as he may require for the purposes of paragraph (a); or (c) be entitled to require any person in possession of decryption information to grant him access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence	problems have been neatly tackled by giving the powers to the police officer itself and nature of obligations for assistance has been enlarged by incorporation of the words 'technical and such other assistance' in subsection b(ii) of this section apart from 'decryption information' in subsection ©. This appears to be the only approach which is likely to work and **it is proposed that necessary amendment in section of the IT Act may be made accordingly.**
15(2)	This section shall apply to a **computer** which a police officer or a person authorised in writing by the Commissioner of Police has reasonable cause to suspect is or has been in use in connection with any offence under this **Act** or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section	Powers of search in investigation apply to only those places/ documents, which are suspected to be involved in the commission of crime. Hence this provision is already contained in CrPC. There is no need for any amendment.
15(3)	The powers referred to in paragraphs (a) (ii) and (iii) and (c) of subsection (1) shall not be exercised except with the consent of the Public Prosecutor	In India, there is no role of public prosecutor during the stage of investigation. The only rationale for the involvement of Public Prosecutor for search of computers and especially requirement of obligation to provide assistance in decryption could be to have some credible supervision. **This could be achieved by entrusting this power in India to Superintendent of Police.**
15(4)	Any person who obstructs the lawful exercise of the powers under subsection (1) (a) or who fails to comply with a request under subsection (1) (b) or (c) shall be guilty of an offence and shall be liable on conviction to a fine not	This provision provides teeth to the obligatory requirement to provide 'assistance' in earlier subsections of this section. Such a provision exists in section 69(3) of IT Act also. **Hence as long as amendments mentioned earlier are incorporated in the IT Act, there is no further requirement for any**

	exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both	**other amendment in this behalf.**
15(5)	For the purposes of this section –	
	"decryption information" means information or technology that enables a person to readily retransform or unscramble encrypted data from its unreadable and incomprehensible format to its plain text version;	This term has not been defined anywhere in the IT Act, although the term finds mention in section 69 (2) of IT Act. Although, the term is self explanatory in computer parlance, **it will be desirable to include this definition in section 2(1) of the IT Act.**
	"encrypted data" means data which has been transformed or scrambled from its plain text version to an unreadable or incomprehensible format, regardless of the technique utilized for such transformation or scrambling and irrespective of the medium in which such data occurs or can be found for the purposes of protecting the content of such data;	This term is not defined in the IT Act, though it has been defined in the proposed Communications Convergence Bill vide section 2 (11). **Hence there is no need for any amendment in this regard.**
	"plain text version" means original data before it has been transformed or scrambled to an unreadable or incomprehensible format	This term is not defined either in the IT Act or in the proposed Communications Convergence Bill. The meaning of this term is self-explanatory and similar to 'decrypted information'. Moreover, this term is not used in the IT Act and **there is no need for any amendment in this regard.**
16	Any police officer may arrest without warrant any person reasonably suspected of committing an offence under this **Act**	Whatever offences are created by the IT Act under chapter XI of IT Act and most of the offences in IPC (as amended by the IT Act) covering computer-related crimes are cognizable offences by virtue of section 468 of CrPC, meaning thereby that a police officer (above the rank of DySP) may arrest without warrant and **hence there is no need for amendment in this regard.**

Comparative Study with Recommendation of the Council of Europe's Convention on Cyber Crimes

Council of Europe Convention on Cyber Crime	Indian Law connected with Computer Related Crimes
Chapter I – Use of terms	
Article 1 – Definitions	
For the purposes of this Convention:	
a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;	The definition of "Computer System' as per section 2(l) of the IT Act, 2000 has all the ingredients contained in the definition of 'Computer System' in the Convention.
b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;	The definition of "Computer Data' as per section 2 (o) of the IT Act, 2000 has all the ingredients contained in the definition of 'Computer Data' in the Convention.
c "service provider" means:	
i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;	The term 'Service Provider' has not been defined in the IT Act anywhere. However, as per section 79, Explanation (a) of the IT Act, 'Network Service Provider' is meant to be 'An Intermediary' as defined in section 2 (w) of the Act. However, as mentioned in para-27 of the commentary to the Convention, the term "Service Provider' does not include 'a mere content provider' whereas he is strictly not excluded from the definition of the 'Intermediary' in the IT Act. As service providers are excluded from certain liabilities as per sec. of the IT Act, **the definition of 'Intermediary' needs to be more exhaustive and exclusive.** This will also clarify the issue of the rights that intermediaries enjoy such as blocking of services for non-payment of rents etc. and avoid such confusions as arose in the case 'State vs. Amit Pansari and Kapil Juneja' of Delhi Police.

d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Since IT Act does not deal comprehensively with procedural aspects, the only option is to rely on the CrPC. However in the changed technological environment of computer related crimes, the same is not sufficient. IT Act does not define the term 'Traffic data' anywhere. The concept of 'Traffic Data' is very important in computer related crimes as being less intrusive than 'Content data' but at the same time extremely important for an investigator. Therefore a more lenient and expeditious procedure has to be laid down wrt the its preservation and disclosure. Secondly, the term has to be defined 'exhaustively' as has been done in the Convention, and not inclusively to avoid any confusion especially as the as there is likely to be lesser supervision of judicial/ quasi-judicial authorities in ordering its preservation and disclosure as compared to 'Content data'. **Hence, there is a need to define 'Content data' exhaustively in the IT Act and lay down criterion for its preservation and production by the 'Service Providers'- on receipt of orders and in some cases on their own.**

Substantive Law: The elements of criminal jurisprudence i.e. 'Intent' and 'without right' form the core of the substantive criminal law in the Convention. However, same is not the case in section 43 of the IT Act, where harmful intent is not an ingredient and the same needs to be rectified.

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

Title I deals with the Computer Crimes in which the Computer System is the target of the offences. The Convention views such offences as offences against the confidentiality, integrity and availability of computer data. This approach is very sound as from the **user point of view, confidentiality, integrity and availability of computer data are the only uses of computer system and any computer crime has to have its intended harm to affect one or more of these three factors. Any future Computer Crime legislation in India can adopt this logic for evaluation and categorization of Computer Crimes in which the computer is a target.**

<u>Article 2 – Illegal access</u>

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.

Mere <u>unauthorized</u> access to a computer system is a civil wrong as per section 43(a) of the IT Act. Further, section 70 of IT Act makes it a criminal offence to secure access to a 'PROTECTED' system. In both these offences, dishonest intent is NOT an ingredient. Sections 43 (b) to (h) covers further civil wrongs, which have the wrongful harm along with illegal access as a prerequisite. **Mere unauthorized access sans any requirement of dishonest intent, specially in case of computers which are not notified to be protected computers is likely to give rise to absurd/ frivolous litigation and therefore section 43(a) should be amended to incorporate the ingredients suggested by the Convention, i.e. infringement of security measures/ dishonest intent/ networked computer.** This is also in consonance with OECD view.

<u>Article 3 –Illegal interception</u>

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its

This section aims to protect PRIVACY of NON PUBLIC TRANSMISSION of computer data while in transit in a technological neutral way i.e. including electromagnetic transmissions. Hence not only interception of 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 electromagnetic 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.

computer data but also interception of fax, telephone, email or file transfer is also covered. Requirement of Interception by TECHNOLOGICAL means is a restrictive qualification to avoid over-criminalisation. **In India traditionally, emphasis on 'privacy' has been missing and there is no separate legislation on privacy except that it flows from article 21 of the Constitution of India. In the IT Act, there is no parallel provision to protect the privacy of data in transit. Section 43 (b) of IT Act deals with 'downloading, copying or extraction of data', which is not only technology specific but also specifically not covering data in transit. Hence it is recommended that Illegal interception of data should specifically be made a separate offence in a technology neutral way owing to rapid advances in communication technology and its convergence with computer technology. To prevent over-criminalisation, the offence should have the requirements of dishonest intent, without right, non-public transmission and use of technological means for interception.**

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.

This protected legal interest in this section is the integrity and proper functioning or use of stored computer data or computer programs. Accordingly, input of malicious codes such as viruses and Trojan horses is also covered in this section as it results in modification of data. In the IT Act, the same legal interests are protected vide sections 43 (c) & (d) as well as Section 65 (Computer Source documents) and section 66 (Hacking). **However, the option given in subsection (2) of this section in the Convention, whereby applicability of this section has been made conditional on the resulting of SERIOUS HARM merits consideration to avoid over-litigation. This could be adopted by either protecting data and programs stored in PROTECTED SYSTEMS only or penalizing only those acts which result in serious damage either wrt monetary value of damage or the sensitivity of data/ programs targeted.**

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.

The protected legal interest of this section is the interest of operators and users of computer or telecommunication systems being able to have them function properly. The denial of service attacks, spamming etc. can be covered under this section. In the IT Act, Sections 43(e), (f), (c) provide similar protection, although they are civil wrongs. However it is recommended that the practice of 'SERIOUS HINDRING' sound legal concept, which should be adopted in IT Act also to avoid frivolous litigation.

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

This section aims to penalize the production, distribution, making available, possession etc. of the tools of crime (e.g. hacker tools etc.), which can be used to commit offences of Illegal Access, Illegal Interception, Data Interference & System Interference. There is no parallel section in the IT Act except for making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii 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 through 5; and

b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

section 43 (g) in a limited way and sections 120B (Criminal Conspiracy) and section 34 (Common Intention) and sections 109-120 of the Indian Penal Code. However, these provisions will be applicable only in respect of a particular offence that has been committed but do not per se prevent proliferation of tools of crime. To draw an analogy, while a person producing illicit weapons may be booked in a murder case, but production of illicit weapons is also an offence in itself. **Hence it is recommended that in order to curb the possession and proliferation of 'TOOLS OF CRIME', this section may be incorporated in the IT Act with sufficient protection for dual-use devices and incorporation of 'specific intent' requirement. Alternately scope of 43(g) may be enlarged.**

Title 2 – Computer-related offences: The Title 2 offences address the computer-related offences, i.e. ordinary crimes that are frequently committed through the use of a computer system. As per the Convention, if the existing laws of a country cover these offences in the cyber environment, there is no need for fresh enactment.

Article 7 – Computer-related forgery

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 input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

This offence is analogous to the offence of 'Forgery' relating to 'documents' in section 463 of IPC as all the ingredients mentioned in the Convention are covered in this section, except for the inclusion of the words, 'electronic record' along with documents. This has also been achieved by amendments to IPC made by the Act read with definition of the 'electronic record' vide section 2(t) of the IT Act. Hence there is no need for enactment of any new section in this regard.

Article 8 – Computer-related fraud

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 person 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 person.

This Section in the Act aims to cover such offences as credit card fraud, electronic fund fraud etc. Although there is no separate section to cover fraud in either IPC or the IT Act, the broad ingredients of this offence in the Convention are covered by section 420 of IPC (which is neutral to the modus-operandi of deceiving) and offences of forgery resultant to the definition of forgery vide section 463 of IPC as amended by the IT Act. Additionally, civil wrong in terms of section 43(h), which covers offences such as credit card frauds also covers 'Fraud' defined by this section of the convention. Hence there is no need for enactment of any new section in this regard.

Title 3 – Content-related offences

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

This section of the Convention aims to address the menace of child pornography, which is specially a problem in the West. The section seeks to cover production (i.e. **addressing the supply side**), offering or making available **(through actual pornographic sites or through hyperlinks)**, distribution or transmission, procuring for oneself or another (**downloading**) and possession (**addressing the demand side**). It is not relevant whether 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 person;

e possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "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, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

the conduct depicted is real or simulated and the images may also be morphed. Thus the section tries to protect the abuse of child as well as criminalize the behaviour that encourages or seduce children into such acts. In India, section 292 of IPC covers obscene literature. Since this section did not cover images in electronic form, therefore a separate section 67 was enacted in the IT Act which criminalizes 'Publishing' and Transmission' of LASCIVIOUS material. The ingredients of offensive subject material in this section remain the same as in section 292 of IPC. Section 67 is not child pornography specific but covers all type of pornography including child pornography. **However the acts 'Publishing' and 'Transmission' may not cover the important act of 'Offering or making available' and hence the scope of section 67 of IT Act can be broadened.** 'Procurement for oneself' or 'Possession' is not criminalized under section 67 of IT Act, nor were these acts criminalized under section 292 of IPC. This approach is not only allowed by the Convention also but has a lot of merit especially due to chances of over-criminalization because of domain name confusions (whitehouse.com is a pornographic site), deep links etc. adopted by porn site owners to trick innocents. The Indian approach has the inbuilt merit that it covers unreal, morphed images also as involvement of real persons is not mentioned specifically. Hence minor amendment to include 'Offering and making available' in section 67 of IT Act would suffice.

Title 4 – Offences related to infringements of copyright and related rights

Article 10 – Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to

In India, the Copyright and Trade-Related Aspects of Intellectual Property Rights are covered effectively by the Copyright Act, 1957 (as amended in 1994), the Designs Act 1911, the Patents Act, 1970 (as amended in 1999) and the Trade and Merchandise Marks Act of 1997 repealing the earlier Act of 1958.

the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Besides, India is a signatory to the Bern Convention, TRIPS and WIPO also and effectively addresses all copyright issues, providing civil and/or criminal liability in appropriate cases. Hence no amendment is required.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be

'Attempt' and 'Aiding or abetment' is already substantive offences under various sections of IPC. **Attempt is covered under section 511 of IPC for attempting to commit**

necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2 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, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**offences under IPC and hence may not cover all offences in the IT Act (as it exists and along with proposed amendments). Therefore, a separate section analogous to section 511 of IPC and the present section of the Convention for attempt needs to be legislated. Additionally, attempt for only Illegal Interception, Data Interference, System Interference and Section 67 of IT Act need to be criminalized as the rest of the offences are either covered in IPC or are not realistically possible to attempt with any appreciable effect without committing.** Abetment is covered in section 109 to 111 of IPC and since it is not tied to offences in IPC alone will cover all offences under any Act. Aiding is also covered partly by section 43(g) of the IT Act. Hence no fresh section needs to be legislated in this regard.
Article 12 – Corporate liability	
1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a a power of representation of the legal person; b an authority to take decisions on behalf of the legal person; c an authority to exercise control within the legal person. 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in	Section 85 of the Act (Offences by Companies) addresses each and every issue addressed in this section and does not need any addition/ amendment.

accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

1 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 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.

2 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.

Punishments and fines under the IT Act are already effective, proportionate and dissuasive, both for natural persons and for legal persons and the **trend is recommended for continuation for new proposed offences.**

Procedural Law:

Rapid strides in Information Technology, which has led to emergence of new forms of crime as well commission of existing crimes, necessitates the **evolution of procedural law to keep pace with the technology. The issues involved are difficulty in identifying the perpetrator and extent of damage in the networked environment, volatility of data, need for secrecy in investigation of online activities and need for expedited preservation of data. DATA CAN BE CATEGORIZED INTO THREE CATEGORIES- TRAFFIC, CONTENT AND SUBSCRIBER DATA WHICH MAY EXIST IN TWO FORMS- STORED OR IN THE PROCESS OF COMMUNICATION. Different criterions need to be evolved for the preservation and production of different types of data in different states depending on the privacy issues involved, volatility, frequency of requirement and importance in investigation. At the same time, privacy and other human rights safeguards need to be addressed. ANOTHER IMPORTANT ISSUES THAT NEEDS TO BE INCORPORATED IN THE LEGISLATIONS IS TO REALIZE THAT PROCEDURAL POWERS MUST RELATE TO ALL FORMS OF DIGITAL EVIDENCE- WHETHER RELATING TO INVESTIGATION OF COMPUTER CRIMES, COMPUTER RELATED CRIMES OR CRIMES IN WHICH DIGITAL EVIDENCE IS INVOLVED IN ANY WAY.**

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 provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

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:

i is being operated for the benefit of a closed group of users, and

ii 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

This Section in the Convention very important principle that powers and procedures with respect to collection of digital evidence to all cases involving digital evidence- computer crimes, computer-related crimes and cases where collection of digital evidence is necessary. **Hence it is recommended that special procedural powers granted already (and those recommended in ensuing paragraphs) should not be limited to offences under the IT Act alone but instead cover all cases involving digital evidence. Secondly, this section underlines the principle that Traffic data is less invasive than content data and therefore power of its preservation, interception and production need to be less stringent than content data. It is recommended that IT Act must also recognize this distinction and provide for more liberal powers for ordering preservation of traffic data to field level functionaries such as Superintendents of Police. Thirdly, although, States are empowered to exempt non-public service providers from orders of preservation etc., in India, because of existing similarity between obligations of public and private service providers, there is no need to make this exemption.**

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.

Article 15 – Conditions and safeguards

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, the 1966 United Nations International Covenant on Civil and Political Rights, 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 procedure or power concerned, *inter alia,* include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

This section addresses the issue of balancing of requirements of investigatory powers with the issues of human rights and privacy issues (**preservation vs. production of data**); proportionality of powers given and need for supervision and control of powers by judicial/ administrative authorities. This is already taken care of in the IT Act so far and it is recommended that it should be continued. **The important point is that proportionality of supervision or power must be balanced with the requirement of an investigator and privacy issues involved and too much upward delegation (e.g. Section 68 and 69 of IT Act, wherein power has been concentrated in the controller) should be avoided.**

Title 2 – Expedited preservation of stored computer data: Article 16 and 17 apply to STORED DATA that has **already** been collected and retained by Data holders such as service providers. These articles apply to data preservation (data which already exists in stored form) and not to retention (data that is currently being generated). Further, these articles try to manage within the existing capabilities of service providers and not to require them to create new facilities. Further, there is a clear distinction between power to order preservation of data (which addresses the volatility issue) and disclosure (which addresses the intrusion of privacy issues)

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles

The section requires that power to order EXPEITED PRESERVATION OF STORED COMPUTER DATA of any type. Considering its vital importance of volatile data, that may otherwise disappear subsequently, this power is extremely important in cases involving digital evidence. Further the power to order preservation has to be given for a specified duration to enable the authority ordering preservation to procure administrative/ judicial orders for its disclosure. **This power is ambiguous in the present day context in India. The situation can be addressed in two-step approach. Firstly, Service Providers/ Intermediaries can be made liable to store certain kind of data (e.g. traffic data) for a specified period (e.g. 180 days) in respect of all communications. Secondly, as intrusion of privacy in case of stored data is minimal and data is very volatile, therefore, the power to order preservation should be given to field level functionaries such as Superintendents of Police. Privacy issue can be addressed by giving the power of order disclosure to a separate Judicial/ Administrative authority. In order to maintain confidentiality of investigation, the data holders must also be liable to maintain confidentiality upto a specified period of time. This will also help in maintaining the privacy of the data subject. These powers need to be specifically provided through amendment of CrPC by broadening the scope of 91 CrPC and inclusion of a new section in CrPC along with suitable amendment in conditions of licences og**

14 and 15.

Service Providers..

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
  a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
  b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Traffic data also does not involve much intrusion of privacy. At the same time, its expedited preservation is vital especially due to its ephemeral nature. **Therefore the suggested amendments wrt this article remain the same as above. However another requirement that needs to be incorporated is that pursuant to a specific order of preservation of traffic data to a service provider, it should be mandatory for a service provider to PARTIALLY disclose traffic data which establishes previous and next links in the communication chain to enable the investigator to take necessary action wrt those links.**

Title 3 – Production order
Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
  a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and
  b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

As opposed to orders of preservation, this section requires the legislation of powers to authorize competent powers to order PRODUCTION IN A SPECIFIED MANNER of **STORED COPMPUTER DATA** or SUBSCRIBER INFORMATIO, which is already in the possession of the data holder. These types of powers are proposed to be given as a substitute to powers of SEARCH AND SEIZURE, which are more intrusive. **It is proposed that firstly, the law in India should clearly define the subscriber information and then create a liability for the service providers to retain all subscriber information. Secondly, the power of production of stored computer data and subscriber information needs to**

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 – Search and seizure of stored computer data

Article 19 – Search and seizure of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a a computer system or part of it and computer data stored therein; and

b a computer-data storage medium in which computer data may be stored in its territory.

2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the

be clearly delegated to authorities in such a manner that privacy issues and requirements of investigation are both met. Subscriber information can easily be made part of section 91 CrPC whereas production of stored computer data can be subjected to the control of order of executive/ judicial magistrate pending which, the data holder should be liable to retain data irrespective of the length of time involved.

In India, the law relating to search and seizure is contained in CrPC and in the absence of any specific provisions in this regard in the IT Act (except that the power is vested in a police officer not below the rank of a Dy. SP of Police vide section 78 of IT Act), the same shall apply in respect of searches and seizures of computers in all cases involving digital evidence also. **Whereas the powers available to police officers as per CrPC in India for conducting a search (including warrantless search under section 165 of CrPC) are very wide, special provisions need to be enacted regarding search of computers due to peculiarities involved in this regard. Therefore, firstly it is recommended that in section 2 of IT Act, it should be included that 'seizing in case of electronic data also includes 'COPYING and/or RENERING INACCESSIBLE (say by encryption)'. Additionally, a distinction** search or similar accessing to the other system.

3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

c maintain the integrity of the relevant stored computer data;

d render inaccessible or remove those computer data in the accessed computer system.

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

has to be made that search of computers for data will follow the norms of 'SEARCH OF CLOSED PLACES' IN CASE OF 'STORED DATA' AND 'TELEPHONE TAPPING' IN CASE OF 'DATA IN TRANSIT'. Since search of computers of ISPs will reveal a lot of data, which is strictly in transit (unopened emails for example), it also needs to be clarified whether 'CLOSED PREMISE' rule or 'INTERCEPTION' rule is to be applied in this respect. Search in a networked environment may also entail accessing of data from another computer through the computer being searched. This other computer resource may be outside India, which involves international issues. In these indirect searches, the issue of notifying the owner of the other computer resource is also involved. Section 69 of the IT Act also need to be amended in two ways in light of para 4 of this section of the Convention. Firstly, the power should not be restricted to 'decryption' alone but should also include other assistance like 'operating system, passwords, hardware locks etc'. Secondly, this power should be given to the person conducting the search and restricting it to the Controller may be impractical.

Title 5 – Real-time collection of computer data: Requirement of real time interception of traffic and/or content data, by service providers/ competent authorities in a CONFIDENTIAL manner is inevitable in Computer Related Crimes. Since privacy interests in content data are higher as compared to traffic data, therefore, stricter criterion can be applied in respect of interception of content data in two ways- limiting the power to higher-level judicial/ administrative/ law enforcement officers and limiting the power to only serious specified category of cases only.

Article 20 – Real-time collection of traffic data

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

a collect or record through the

The requirement laid down by Para 1and 3 of this section need to be adopted in totality. At present, under the IT Act, there is no distinction between the Traffic data and Content data and the power to order application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party; or

ii to co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

interception is given only the Controller as per section 69 of the Act. This power is also limited to direct only a Government agency to intercept data. **It is recommended that firstly, the power to order interception of traffic data should be vested in an administrative authority such as Home Secretary on the lines of telephone tapping under section 5(2) of the Indian Telegraph Act. Moreover, as traffic data is less intrusive than content data, this power should be vested in a District magistrate. Alternately, we can follow a two step approach- power to order interception can be given to SP and power to order disclosure to DM. Secondly, this power should be applicable on ALL SERVICE PROVIDERS- whether public or Govt.. Thirdly, the person ordered to intercept the information must be under obligation to maintain CONFIDENTIALITY. These provisions need to be specifically incorporated in the IT Act.**

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

The requirements and amendments proposed for implementation of this article are the SAME AS THE PREVIOUS ARTICLE, i.e. interception of traffic data except that in this case, the authority who can be vested with the power to order interception can be vested in a higher authority than that required in case of traffic data or power to order interception can be vested in SP/DM but power to order disclosure of intercepted

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

information can be vested in a judicial authority.

Section 3 – Jurisdiction
Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a in its territory; or

b on board a ship flying the flag of that Party; or

c on board an aircraft registered under the laws of that Party; or

d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the

The sub-article 1(a),(b) & (c) reiterate the 'Principle of Territoriality' in invoking jurisdiction which is already in existence in India and further extended by section70 of IT Act.

Sub-article 1(d) reiterates the 'Principle of Nationality'. It provides that nationals of a State are obliged to comply with the domestic law even when they are outside its territory. This principle finds place in section 4(1) of IPC.

territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

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 the 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.

This concession is not required by India.

This paragraph underlines the principle 'aut dedere aut judicare' i.e. 'extradite or prosecute'. Subjected as it to the jurisdictional concepts in paragraph 1 above, this principle is essential for international cooperation and recommended for acceptance.

This paragraph gives validity to extra-territorial jurisdiction invoked by section 70 of IT Act.
Does not need any comments. Appears to be an acceptable course of action.

This Article underlines three important principles namely ' cooperation to the widest possible extent', 'cooperation based on international instruments, reciprocal arrangements and in accordance with principles enumerated in this section' and 'cooperation in the investigation of all computer related crimes and cases involving digital evidence'. The last principal again emphasizes that irrespective of whether the offence is a computer-related offence or otherwise, the same principles of cooperation need to be applied as long as electronic evidence is involved. This is a reiteration of provisions of Art 14 and should be accepted by India.

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 through 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.	Usual conditions for extradition i.e. 'Dual Criminality' and 'Minimum term of imprisonment' have been incorporated in this paragraph. Ait should be acceptable except that minimum term of imprisonment can be stipulated to be two years as per prevailing practice in India.
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 (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.	Needs no comments in light of comments made supra.
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.	This appears to be a rational approach. Extradition treaties can either be 'offence specific' or 'omnibus'. Wherever we have offence specific extradition treaties, we should incorporate offences mentioned in this Convention (subject to comments made for each offence already) in the treaty. In omnibus extradition treaties, there should not be any problem as long as conditions of 'dual criminality' and 'minimum term of imprisonment' are satisfied.
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.	No comments except that if India becomes a signatory to this Convention, it MAY consider THIS convention as a notional extradition treaty in respect of other signatories. No comments as does no apply to India.
4	Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between	Reiterates only the accepted international practice and hence should be acceptable to

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 for 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 address of each authority responsible for making or receiving requests 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.

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

India.

This paragraph outlines the procedure in case extradition is refused either on the basis of nationality of the criminal or assumption of jurisdiction by the Requested Party. The course outlined in this paragraph is the only logical manner to proceed against the criminal. Moreover, it does not violate any criminal law in India. Hence it should be acceptable to India.

Does not need any comments.

Does not need any comments.

Does not need any comment except that international cooperation is required for investigation of all types of offences involving 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.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.

4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence, which it considers a fiscal offence.

5 Where, in accordance with the

collection of evidence in electronic form i.e. the paragraph reiterates the principle of Article 14.

No comments.

Generally all requests in international arena follow a very formalized procedure, which is legally intensive, secure, authenticated and at the same time time-consuming. The nature of investigations dealing with collection of evidence in electronic form being such where any delay in communication of request might be fatal, this paragraph prescribes an alternate procedure for making expedited but secure and authenticated requests. **There does not appear to be any other way to deal with cyber crime and hence India should be supporting this clause.**

This Convention is an 'Integrated Package' i.e. subject to discretions provided in the Convention, a Party either accepts the whole Convention or rejects it. That being the case, it follows as a corollary that computer-related offences vide articles 2-11 of this Convention have been deemed to be accepted by the Signatories. Thereafter, subject to any limitations in the existing International agreements/ extradition treaties, the Convention forbids refusal of mutual assistance for offences specified in this Convention by terming them as 'fiscal offences'. **This prevents the sabotaging of the spirit of widest possible cooperation envisaged by the Convention and thereby ensures that mutual assistance is not denied on flimsy grounds. This should be acceptable to India.**

This Paragraph recognizes another reality i.e. same criminal misconduct may be categorized differently in different countries and that might be used as a pretext for denying mutual assistance and therefore prohibits such a practice.

This again seeks to prevent sabotaging of

provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

the spirit of widest possible cooperation envisaged by the Convention and thereby ensures that mutual assistance is not denied on flimsy grounds. This should be acceptable to India.

Article 26 – Spontaneous information

1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.

2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

Needs no comment as firstly the provisions are not obligatory and secondly, they have a very novel intention behind them. Such an exchange does take place, especially between the intelligence agencies of different nations.

Title 4 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force

As mentioned earlier, the Convention proposes the mutual Cooperation regime as per the existing multilateral/ bilateral between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c 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 names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the

international arrangements or extradition treaties, wherever they exist already, in order to maintain status quo. However, wherever they do not exist, this Article outlines the procedure and conditionalities to achieve the widest possible mutual assistance within the ambit of sovereignty.

Provisions of this Article SHALL apply only under two conditions:

Firstly, if no mutual assistance treaty already exists. OR

Secondly, if they exist, both the countries agree to implement these provisions.

Hence, if we do not have any mutual assistance treaty with a particular signatory, then provisions of this Article SHALL be binding on us.

Such Central/Nodal Authorities are essential for expedited execution. CBI, the nodal agency for Interpol related requests, can perform this function also.

Needs no comments. Essential requirement for expedited communication.

Needs no comments.

Needs no Comments.

Within the safeguard of 'incompatibility', the investigating authority (and hence Requesting Party) must have the prerogative as to how the request should be executed w.r.t. requirements of investigation and hence we should not have any problem in accepting this proposition.

These are the normal safeguards that need to be extended in any international request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions, as it deems necessary.

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police

Convention to protect the sovereignty of the Signatories.

The Convention gives precedence to 'Domestic' investigations over 'Requested Assistance' in similar circumstances and thereby recognizes the sovereignty principle.

Needs no comments, as it is naturally agreeable course of action in case of difficulty in acceding to request wholly.

Needs no comments, as it is naturally agreeable course of action in case of difficulty in acceding to request wholly.

Needs no comments, as it is naturally agreeable course of action in case of difficulty in acceding to request wholly.

Needs no comments. The provision does not have any pitfall and we should accept it.

Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

Needs no comments.

Needs no comments.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

Needs no comments except that in international communication, communications through a nodal agency is always a preferred route.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Needs no comments.

Article 28 – Confidentiality and limitation on use

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

Under the Convention, existing International arrangements, agreements and Treaties etc. take precedence in matters of mutual assistance. **Hence this should be acceptable to every nation, as it does not impose any new obligations.**

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or

b not used for investigations or proceedings other than those stated

However if such an arrangement does not exist, then Requested Party has the right to impose conditions subject to which information asked for shall be supplied by it These conditions are mentioned in Article 20(2)(a) & (b) and are aimed at protecting the sovereign interests of the Requested Party. **Hence we should not be having any reservations in accepting the same.** Moreover, such conditions are generally in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

included in other extradition treaties as a matter of routine.

It may not be possible for a Requesting Party to adhere to the conditions mentioned supra (for example evidence may have to be made public during trial) and in that case, what needs to be done by both the parties is outlined in this paragraph. **We should not be having any reservations in accepting the same.**

Follows as a natural corollary of Paragraph 2. Needs no comments.

Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29– Expedited preservation of stored computer data

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

This proposition is unavoidable in the context of technology involved in investigation of Computer-Related Crimes. It is a well-known fact that the formal procedures of making request to other countries such as 'letter rogatory' will not suffice owing to volatile nature of computer data. Consequent to preservation of data on request, a formal request can be awaited for disclosure subject to any judicial scrutiny of the request. Till that time, the requested party may not be required to take custody of the data from the custodian. **However in order to implement this provision, we have to delegate the power to order preservation and interception, besides search and seizure on international requests, to executive officers such as Superintendents of Police of the Nodal Agency such as CBI, without any judicial intervention at that stage.**

2 A request for preservation made under paragraph 1 shall specify:

This is intended to make requests very specific so that firstly they assure the

- a the authority seeking the preservation;
- b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
- c the stored computer data to be preserved and its relationship to the offence;
- d any available information identifying the custodian of the stored computer data or the location of the computer system;
- e the necessity of the preservation; and
- f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, **dual criminality shall not be required as a condition to providing such preservation.**

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

requested party of the genuineness of the request and secondly that the request can be complied with.

It must be recognized that merely for the purpose of preserving data, the precondition of proof of dual criminality will be counter-productive as the procedure is legally intensive and time consuming. However, before disclosing the data, the condition of 'dual criminality' can be imposed.

The Convention indirectly imposes a condition that dual criminality is automatically assured for offences under the Convention. However, Parties may refuse requests for offences outside the Convention, if the requested Party thinks that the Requesting Party shall not be able to meet the criterion of 'Dual Criminality' at the time of disclosure.

This is an important leeway provided to Parties to refuse 'Preservation'. The concession is based on well-accepted principles of sovereignty and should be able to meet the aspirations of India.

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

This provision is incorporated to give advance warning to Investigators so that they can search for alternatives which may be more intrusive but safer- such as production order, search and seizure requests etc. This should be readily agreed to.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Since legal procedures of making formal international requests are very long and time consuming, therefore, the minimum time limit that has been imposed is reasonable and should be acceptable to us.

Article 30 – Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

This provision is extremely important in domestic as well as international jurisdictions. Essentially, this obligation to disclose necessary traffic data, which discloses links in communication chain, must be enforced upon the Service Providers. Once they disclose these links, they must be communicated to the Requesting party to enable it to take further necessary action. Hence, this paragraph essentially reiterates Paragraph 17(1)(b) in an international scenario and hence should be acceptable to India.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or

b the requested Party considers that execution of the request is likely to

This paragraph provides the concessions normally required to protect the sovereignty of signatories and should be acceptable to India.

prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 – Mutual assistance regarding investigative powers

Article 31 – Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.

2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.

3 The request shall be responded to on an expedited basis where:

a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or

b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

The proposition made in this article is wholly acceptable, desirable and essential for a war on Cyber criminals. The law in India needs to give powers to Nodal Agency Officers to carry out these requests on the same lines as if the powers were to be executed for a domestic case.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party

Subject to the conditions that the data is an 'open-source' data, or the requisitioning Party has taken consent from the **lawful** custodian of data, there is no reason to disagree with the proposition. In case of open source data, the data is anyway in public domain and if we agree to this principle, it only makes that data legally admissible.

through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data.

1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.

2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Agreed as without mutual assistance in real time collection of traffic data in the cyber world, it is not possible to deal with cyber crimes. The powers in this regard need to be delegated to field level officers on the same lines as in the case of domestic cases. However, the procedure can be subjected to same conditionalities as exist in domestic law.

Article 34 – Mutual assistance regarding the interception of content data

The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Agreed as without mutual assistance in real time collection or recording of content data in the cyber world, it is not possible to deal with cyber crimes. The powers in this regard need to be delegated to field level officers on the same lines as in the case of domestic cases. However, the procedure can be subjected to same conditionalities as exist in domestic law.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-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 the following measures:

CBI can act as a nodal agency in this regard, on the same lines as it is already a nodal agency for Interpol purpose. **However, it goes without saying that this nodal agency must be vested with powers to order interception of data and preservation of traffic logs (header information) directly, without seeking permission from any judicial authority as said earlier. However at the time of disclosure, a judicial scrutiny will not be a hindrance in international cooperation.**

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision 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.

Specifications for Write-block Tool and Disk Imaging Tool

Accurate and dependable forensic tools are required for a reliable means of investigating crimes that involve computers.

The specifications are based on the guidelines issued by US Department of commerce through one of its agencies (National Institute of Standards and Technology)

GLOSSARY

i. Bit-stream duplicate: a bit-for-bit digital copy of a digital original document, file, partition, graphic image, entire disk, or similar object.

ii. Checksum: a hash computed from a specific computational algorithm, such as the Cyclic Redundancy Checksum 32-bit (CRC-32).

iii. Disk compares equal: a bit-stream duplicate is compared to the original digital object and no differences are found.

iv. Disk compares qualified equal: a bit-stream duplicate is compared to the original digital object and the only differences found are those documented as different by the tool that created the bit-stream duplicate or image from which a bit-stream duplicate was reconstructed. (See "qualified bit-stream duplicate".)

v. Duplicate: a copy of an original object.

vi. Hash: A function that maps keys to integers, usually to provide an even distribution of keys on a smaller set of values. A coded number or string of characters used to represent the value derived from a hash function on the contents of a bit-string, in this case a disk, partition, image, or file contents.

vii. Image: a digital, sometimes compressed, file from which a bit-stream duplicate of an original digital object can be reconstructed.

viii. Qualified bit-stream duplicate: a duplicate except in identified areas of the bit-stream, such that the identified areas are replaced by values specified by a disk imaging tool's documentation, such as partition table entries to reflect relocated partitions; boot records; fill areas required for cylinder alignment, and excess disk space.

Write-Block Tool Specifications

REQUIREMENTS

This section presents mandatory requirements that all write block tools must meet and a list of optional requirements that some write block tools may provide.

Mandatory Requirements

The informal hard disk write block tool requirements are the following:

i. The tool shall not allow a protected disk to be changed.
ii. The tool shall not prevent obtaining any information from or about any disk.
iii. The tool shall not prevent any changes to a disk that is not protected.

The three informal requirements are the essence of a write blocking tool: protect the evidence from alteration while allowing a complete examination of the evidence. A formal statement of these requirements follows:

i. The tool shall block any commands to a protected disk in the write, configuration, or miscellaneous categories.
ii. The tool shall not block any commands to an unprotected disk.
iii. The tool shall not block any commands to a protected disk in the read or information categories.
iv. The tool shall give an indication to the user that the tool is active.
v. The tool shall report all disks accessible by the covered interfaces.
vi. The tool shall report the protection status of all disks.
vii. The tool shall, if so configured, adjust the return value of any blocked commands to indicate that the operation was carried out successfully even though the operation was blocked.
viii. The tool shall, if so configured, adjust the return value of any blocked commands to indicate that the operation failed.
ix. Return values of information commands shall be consistent with return values of any blocked commands. (For example, a command to return status of last command after a blocked command shall return the same value as returned by the blocked command.)

Optional Requirements

The following requirements define optional tool features. If a tool provides the capability defined, the tool is tested as if the requirement were mandatory. If the tool does not provide the capability defined, the requirement does not apply.

i. The tool shall alert the user when a command is blocked, either by an audio or a visual signal.
ii. The tool shall be able to uninstall itself if requested.
iii. The user shall be able to specify a subset of the covered disks for protection.
iv. The tool shall log a subset of command executions that have been blocked.

ASSERTIONS

Each assertion provides a specific class of conditions that can be tested and the result that is expected.

Mandatory Assertions

i. If a disk is protected and a command from the write category is issued for the protected disk then the tool shall block the command.

ii. If a disk is protected and a command from the configuration category is issued for the protected disk then the tool shall block the command.

iii. If a disk is protected and a command from the miscellaneous category is issued for the protected disk then the tool shall block the command.

iv. If a disk is protected and a command from the read category is issued for the protected disk then the tool shall not block the command.

v. If a disk is protected and a command from the information category is issued for the protected disk then the tool shall not block the command.

vi. If a disk is not protected and a command from any category is issued for the protected disk then the tool shall not block the command.

vii. If the tool is executed then the tool shall issue a message indicating that the tool is active.

viii. If the tool is executed then the tool shall issue a message indicating all disks accessible by the covered interfaces.

ix. If the tool is executed then the tool shall issue a message indicating the protection status of each disk attached to a covered interface.

x. If the tool is configured to return *success* on blocked commands and a command is blocked by the tool then the return code shall indicate successful command execution.

xi. If the tool is configured to return *fail* on blocked commands and a command is blocked by the tool then the return code shall indicate unsuccessful command execution.

xii. If the tool is active and a command is blocked and the next command issued is a *return status of last command* then the value returned shall match the value returned by the blocked command.

Optional Assertions

i. If the tool blocks a command then the tool shall issue either an audio or a visual signal.

ii. If the tool is active and the tool is then uninstalled then no commands to any disk shall be blocked.

iii. If a subset of all covered disks is specified then commands from the write, configuration and miscellaneous categories shall be blocked for disks in the selected subset.

iv. If a subset of all covered disks is specified then commands from the read and information categories shall not be blocked for disks in the selected subset.

v. If a subset of all covered disks is specified then no commands from any category shall be blocked for disks not in the selected subset.

If the tool is active and command logging is specified then the tool shall create a log of commands blocked.

Disk imaging tool's specifications:

REQUIREMENTS

The top-level disk imaging tool requirements are the following:

i. The tool shall make a bit-stream duplicate or an image of an original disk or partition.
ii. The tool shall not alter the original disk.
iii. The tool shall be able to verify the integrity of a disk image file.
iv. The tool shall log I/O errors.
v. The tool's documentation shall be correct.

While these requirements appear to be clear and concise, they are rife with implicit requirements and ambiguities. An effort to be more precise is required in order to evaluate how well a particular implementation meets the requirements. Sections 5.1 and 5.2 contain more precise statements of these requirements.

All disk imaging tools shall be able to accomplish the tasks described as mandatory requirements. Optional requirements are tested as if they were mandatory requirements if the tool under test supports the applicable feature. If a specific tool does not provide the capabilities of a particular optional requirement, then the tool is not tested for that requirement. This means that a specific tool might provide none of the capabilities described under optional requirements.

Mandatory Requirements

The following requirements are mandatory and shall be met by all disk-imaging tools.

i. The tool shall not alter the original.
ii. If there are no errors accessing the source, then the tool shall create a bit-stream duplicate or image of the source.
iii. If there are I/O errors accessing the source, then the tool shall create a qualified bit-stream duplicate or image of the source. (A *qualified bit-stream duplicate* is defined to be a duplicate except in identified areas of the bit-stream.) The identified areas are replaced by values specified by the tool's documentation.
iv. The tool shall log I/O errors in an accessible and readable form, including the type of error and location of the error.
v. The tool shall be able to access disk drives through one or more well-defined interfaces.
vi. Documentation shall be correct insofar as the mandatory and any implemented optional requirements are concerned, i.e., if a user following the tool's documented procedures produces the expected result, then the documentation is deemed correct.
vii. If the tool copies a source to a destination that is larger than the source, and it shall document the contents of the areas on the destination that are not part of the copy.
viii. If the tool copies a source to a destination that is smaller than the source, the tool shall notify the user, truncate the copy, and log this action.

Optional Requirements

The following requirements define optional tool features. If a tool provides the capability defined, the tool is tested as if the requirement were mandatory. If the tool does not provide the capability defined, the requirement does not apply.

i. The tool shall compute a hash value of the complete bit-stream duplicate generated from an image file of the original source, compare the computed hash value to the hash value of the original source computed at the time the image was created, and log the results of the comparison on a disk file.
ii. The tool shall divide the destination bit-stream into blocks, compute a hash value for each block, compare the computed hash value to the hash value of the original block of source data computed at the time the image was created, and log the results of the comparison on a disk file.
iii. The tool shall create a bit-stream duplicate of individual partitions as directed by the user.
iv. The tool shall allow the user to view the source partition table and the tool shall log the contents of the source partition table.
v. The tool shall log one or more of the following items on a disk file: tool version, subject disk identification (if the identification is available, such as manufacturer, make, model, serial number, sector count, etc.), any errors encountered, tool actions, start and finish run times, tool settings, and user comments.
vi. The tool shall create an image file on fixed or removable electronic or magnetic media that can be used to create a bit-stream duplicate of the original.
vii. The tool shall create a qualified bit-stream duplicate and adjust the alignment of cylinders to cylinder boundaries of disk partitions on a destination of a different physical geometry. The identified areas of the duplicate that are allowed to be changed are the following: partition table entries to reflect the relocated partitions; boot records; fill areas required for cylinder alignment, and excess disk space. The fill areas shall be given values as specified in the tool documentation.

ASSERTIONS

Each assertion provides a specific class of conditions that can be tested and the result that is expected.

Mandatory Assertions

In the following, wherever source and destination are used without modification, the term refers to both source partitions and entire disks or destination partitions and entire disks. The requirement paragraph related to each assertion is referenced in parentheses.

i. If a source is accessed by the tool, then the source will not be altered.
ii. If there are no errors reading from a source, nor errors writing to a destination, then a bit-stream duplicate of the source will be created on the destination.
iii. If there are errors reading from a source or writing to a destination, then a qualified bit-stream duplicate of the source will be created on the destination. The identified areas are replaced by values specified by the tool's documentation.

iv. If there are errors reading from the source or writing to the destination, then the error types and locations are logged.

v. If the source or destination is an IDE or SCSI drive and an image or bit-stream duplicate is created, then the interface used is presumed to bë among those specified in

vi. If the expected result of any test defined in this specification is achieved and the documentation was followed without change in achieving this result, then the documentation is presumed correct.

vii. If a bit-stream duplicate of a source is created on a larger destination, then the contents of areas on the destination that are not part of the duplicate are set to values as specified in the tool documentation.

viii. If a bit-stream duplicate of a source is created on a smaller destination, then the duplicate is qualified by omitted portions of the bit-stream and the tool will notify the user that the source is larger than the destination.

Optional Assertions

If an implementation provides a capability covered by one or more of the following optional assertions, then tests derived from those assertions will be applied to the implementation.

i. If a hash of one or more blocks (i.e., less than the entire disk) from the source is computed before duplication and is compared to a hash of the same blocks from the destination, the hashes will compare equal. If more than one partition exists on the source disk, the tool will produce a duplicate of any user-selected source partition on the destination.

ii. If a partition exists on the source, the tool will display or log a message indicating that the partition exists and display or log one or more items of information from the following list: drive indicator, device type, device address or mount point, size, space used, and free space.

iii. If the tool logs the tool version, it will be the version referred to in the implementation's documentation.

iv. If the subject disk identification is available and the tool is capable of logging the subject disk identification, then the subject disk identification will be logged.

v. If the tool logs the source partition table in human readable form and the information from the source partition table can be ascertained independently from the tool, then the source partition table information will accurately match the content of the independent partition table information.

vi. If the tool logs errors and any error occurs, then the type and location of the error will be logged.

vii. If the tool logs tool actions and the tool's documentation states what actions are logged, then the actions logged will accurately match those documented in the tool's documentation.

viii. If the tool logs start and finish run times, then the logged start and finish run times will accurately match those recorded by the tester according to screen input images, test input scripts, or tester notes.

ix. If the tool logs tool settings and the tool's documentation states what settings are logged, then the logged settings will accurately match those set by the tester or as documented in the tool's documentation.

x. If the tool logs user comments, then the logged user comments will accurately match those entered by the tester as captured in screen input images, test input scripts, or tester notes.

xi. If the tool creates image files, then it will create an image file of a source on a magnetic medium that can be removed from the platform on which it was created.

xii. If the tool creates an image file from a source on a removable magnetic medium, then a duplicate of the source created from the removable magnetic medium will result in a duplicate on the destination and the destination will compare equal to the source.

If an image file is created, and there are no errors reading from a source, nor errors writing to a destination, then a bit-stream duplicate created from the image file will compare equal to the source.

User Specifications of the Seizure, Acquisition and Analysis Tool

The first phase of the software and the Manual for investigation of Computer related crimes was released on 18th Feburary 2004 by Sh Laksmi Nayayn Addl Secretary department of Information Technolgy MCIT Delhi.

Though there exist a large number of forensics tools, Cybercheck is a Computer forensic tool exclusively written to incorporate the recommended procedure. The following are the specifications which were agreed upon, that the CyberCheck Suite shall Incorporate. Most of the specifications have been meet, and it is hoped that the remaining would be met by the year end. All attempts have been made to make it user friendly, and assist in the analysis procedure with a very user friendly interface.

The tool is based on the following specifications. The version 1 of the software does not provide for all the features, but fulfills the essential requirements for completing the process of seizure, acquisition and analysis of the digital evidence.

The Forensic Tool may be called CyberCheck with the following specifications. It shall have two components

i) A bootable software to be referred as Trueback.
ii) Analysis tool to be referred as Cybercheck.

User Specifications of Trueback Bootable Software

Trueback bootable software should have following features:

I. Storage Medium:
   i. It should be contained on a bootable floppy as well on a CD ROM[1].
II. Components of the software
   i. It should contain software for booting an IBM, IBM Compatible computer system in MS DOS mode.
   ii. Self-authentication[2] feature to conduct self-authentication every time it is run.
   iii. A software which permits accessing the setup, and modifying the booting sequence of the suspect computer after being booted using the Trueback booting software. This component software may be called "Bootwiz"
   iv. A seizure and Acquisition tool called "Trueback" for seizing, and acquiring digital evidence
III. Tureback should be able to acquire all common types of media including hard drives, floppies, CD-Roms, SCSI hard disks, and should support USB interface for seizing other types of storage medias.

Seizure of Evidence:

[1] The most commonly removable storage media. Whereas CD ROMs are less susceptible to damage, CD ROM drives may not be available in all suspect computers. Therefore this software should be available on a 3 ¼ inch floppy also.

[2] Whenever Trueback is run, it should validate itself against the precalculated hash value, which is calculated and stored by the manufacturer in the software itself. In case any discrepancy is found, it should prompt an error message.

I. The seizure tool should
   i. Self-authentication check.
   ii. Capability for write-blocking of all storage media including itself.

II. Have a Graphic Interface requesting for following information:
   i. Name of the Investigation Officer
   ii. Rank
   iii. Date and Time of Seizure
   iv. Place of scene of seizure
   v. Crime No.[3]
   vi. Name of the Police station
   vii. Custodian of suspect computer
   viii. Name of witness 1
   ix. Name of witness 2[4]
   x. Brief Notes

III. Extract the following information from the suspect system, keep it in RAM and display[5] it to the user:
   i. Suspect computer's system date and time[6]
   ii. Suspect computer's MAC address if any
   iii. Suspect computer's configuration[7]
   iv. Details of storage media attached to it including their capacities and serial numbers
   v. Prompt for storage media to be seized[8].
   vi. Display[9] the following information about the selected storage media to be seized:
   vii. Capacity of the drive[10]
   viii. Details of the drive- including serial no.
   ix. Amount of data stored on it[11]
   x. Block size[12] and no. of blocks

IV. Prompts for acceptance and starting of seizure.

[3] Refers to the FIR No.

[4] As per section of Indian Evidence Act, all evidence must be seized in the presence of atleast two, local and independent witnesses.

[5] So that the IO can make a physical note of these details for mentioning the same in the forwarding note to the laboratory for double authentication.

[6] May be different from the actual date and time and this difference shall be vital in analysing the date and time stamps of the evidence.

[7] Details like, storage capacity, etc

[8] In case of multiple storage media attached to a suspect computer, the IO will have too select one media at a time.

[9] For IO to make a physical note of it so that he can enclose this information in forwarding note to the lab for double authentication.

[10] This will decide the capacity of the storage drive on which evidence is stored.

[11] For making a physical note of it by the IO and forwarding the same in the forwarding memo to the lab for double authentication.

[12] Block size will be so calculated so as to optimise minimum loss of data in case of corruption, time taken to seize the data in blocks and the total storage capacity required to store the individual hash values and other details so that total storage capacity requirement should be less than 1.44 MB, the storage capacity of a floppy. The display of this information is required as IO may need to change the block size depending upon the sensitivity of the data being seized.

V. Starting from first sector, sequentially calculates the hash value of each block storing the hash value of each block, its starting and ending sector and the block no. in RAM[13].

VI. On finishing with the last block, calculates the hash value of the whole storage media as well as the hash value of the block hash values[14].

VII. Generates a report consisting of the following and keeps these contents in the RAM

   i. Name of the Investigation Officer
   ii. Crime No.
   iii. Name of the Police station
   iv. Date and Time of Seizure
   v. Place of seizure
   vi. Name of witness 1
   vii. Name of witness 2
   viii. Suspect computer's system date and time
   ix. Suspect computer's configuration
   x. Suspect storage media details
   xi. Total No. of Blocks
   xii. Starting and ending no. of each block and their hash value
   xiii. Hash Values of the whole suspect storage media
   xiv. Hash Value of all the Block Hash values

VIII. Calculates the hash value of the Report[15] mentioned above.

IX. Displays[16] the Entire Hash value of the Suspect Media, hash Value of all the block hash values and Hash value of the Generated Report.

X. Prompts the IO to remove Trueback CDROM/Floppy and insert SSM Floppy.

XI. All the contents of the report and the hash value of the generated report are transferred on to SSM. (Such a floppy may be called CSF- CyberSeize Seizure Floppy)

XII. Repeat[17] the process of creating as many CSFs as the IO wants. A minimum of four such floppies should be made.

XIII. Display the list of remaining storage media attached to the suspect computer, which is yet to be seized and seek instruction for seizure of the next storage media or exit. If the user selects another storage media, delete all previous stored contents RAM before repeating the process of seizure.

XIV. Ability to exit the system and shut down.

[13] There is no storage media on which this information can be stored. Therefore it has to be in RAM.

[14] To eliminate any possibility of backward interpolation of hash values in case of tampering.

[15] To detect any tampering of the report.

[16] To enable the IO to mention the same in the physical seizure memo, which will be signed by the IO, custodian of suspect computer and the witnesses as per section of CrPC and a copy of which will be given to the custodian of suspect computer under receipt. The IO will forward a copy of this physical seizure memo to the lab also.

[17] Multiple copies of CSF are required for sending to lab, handing over to custodian of suspect computer and for record of IO.

Acquisition:

After seizure of the evidence, the evidence would be required to be acquired by a Computer Forensic Analyst in the lab[18] for analysis.

I. Mode of acquisition: Trueback should work both in computer-to-computer acquisition through a parallel port link[19] between the suspect computer and trusted workstation or through drive-to-drive[20] (localmode) acquisition in the trusted workstation environment.

II. Trueback should be able to boot the computer (either the suspect computer or the trusted workstation) and conduct a self-authentication check of booting software, prompting for error and exit in case of any corruption.

III. Write block[21] all storage media connected (directly or through a lap link) with the computer on which Trueback is working.

IV. Display a list of all storage media connected with the system(s)[22] along with their drive specification, storage capacity and status (primary, primary slave, secondary slave etc.)

V. Prompt an Acquisition Wizard seeking the following details:

   a. Name of the Officer acquiring evidence
   b. Date and time of acquisition
   c. Laboratory reference number
   d. Name of evidence file and folder to be generated
   e. Prompt for designation of source and the destination drives (for destination drive should be a SSM HDD)
   f. Prompt for insertion of CSF and after its insertion; conduct its authentication check by comparing its generated hash value with stored hash value. Prompt for error and exit in case of mismatch.
   g. Compare and display[23] source drive details as read from designated source drive and compare it with source drive details contained in CSF. Prompt for error and exit in case of mismatch.
   h. Prompt for starting the process of acquisition. At this stage, the write block of only the destination drive is disabled[24].

Process of Acquisition:

[18] This process would be done in the laboratory only by an expert. Acquisition would be required since it is prohibited to work on original evidence.

[18] Where for some reason, it is not practical to remove the HDD from the suspect computer.

[18] The usual acquisition mode where the suspect HDD is connected as a slave to the Computer Forensic Workstation.

[18] View all drives as virtual drives only for the time being to maintain integrity of evidence.

[18] In case of parallel lap link, this includes the suspect machine in addition to computer forensic workstation.

[18] For comparison with source drive details in Physical seizure memo.

[19] Where for some reason, it is not practical to remove the HDD from the suspect computer.

[20] The usual acquisition mode where the suspect HDD is connected as a slave to the Computer Forensic Workstation.

[21] View all drives as virtual drives only for the time being to maintain integrity of evidence.

[22] In case of parallel lap link, this includes the suspect machine in addition to computer forensic workstation.

[23] For comparison with source drive details in Physical seizure memo.

[24] As imaged data has to be written on to the destination drive.

I. Utilising information contained in CSF, block by block bit-stream imaging on to destination drive.

II. Validation through calculation of block hash value for each block in the source drive and destination drive and comparison of these two with stored block hash value in CSF.

III. Error message (if any) for each block indicating type of mismatch:
   a. Mismatch in CSF and source.
   b. Mismatch in source and destination.
   c. Mismatch in CSF and destination.

IV. Prompt for:
   a. Ignore[25]
   b. Ability to Re-image

V. Continue this process until there is no error or user has selected ignore option in which case the information contained in that block should be distinguishable from other information through colour coating.

VI. At the end of imaging of all the blocks, stitching and authenticate the entire image by comparison of hash value of the entire image with the relevant hash value of source disc as contained in CSF, in case there was no mismatch[26] for any block.

VII. Generation and display of a report containing the following details:
   a. Date and time of acquisition
      i. Start time
      ii. End time
   b. Details of source disc
   c. Details of destination disc
   d. Crime number and name of Police Station
   e. Laboratory reference number
   f. Name of the acquisition officer
   g. Total number of blocks
   h. Number of blocks imaged with authentication
   i. Number of blocks imaged which could not be authenticated; their block numbers, starting sector number and ending sector number.

VIII. Transfer the generated report to the acquired evidence HDD.

Seizure and Acquisition:

This option could be exercised both at the scene of crime (when computer forensic analysts are called to the scene of crime) or at the computer forensic laboratory (when in rare circumstances, the hardware is physically seized without hashing and sent to the laboratory)

I. Scenarios:
   a. Storage media to sterile storage media Using suspect computer motherboard.
   b. Using computer forensic workstation

[25] In case there is any mismatch between the CSF and the source drive, the user can not do anything except ignore and proceed. However, in case of other mismatches, the user tries rei mage the source drive till there is no mismatch or the user ignores and proceeds to the next block.

[26] In case of mismatch, the hash value for the entire image shall not match the hash vale of the entire source (suspect) disk, in any case.

c. Parallel lap link between the suspect computer and computer forensic workstation.

II. After configuration[27] of the system, booting up the system i.e., suspect computer in scenario (i) & (iii) and forensic workstation in scenario (ii). Along with booting, Trueback ensures:

a. Self-authentication check of booting software, prompt and exit in case of corruption.

b. Write blocking of all storage media.

c. Display[28] a list of all storage media connected to the system(s) along with their drive specification, storage capacities and current status[29] and prompt for designation of source and destination drives. The user should be prompted to accept the status before proceeding further or to exit the system for altering the connections to ensure proper master slave configuration.

d. Prompt for Write-Block removal on Destination Drive.

e. Divides the Suspect storage media into optimum no.[30] of blocks.

f. Starting from First Block, starts bit-stream imaging of the entire suspect storage media on to the destination drive, in the following manner:

g. Store the starting and ending sector no. for each block in RAM.

h. Calculates block hash value of a block as stored in suspect storage media and as imaged on to the destination drive and authenticates by compares the two.

i. In case the two hash values match, store the hash value in RAM against the sector nos. for that block.

j. In case, there is a mismatch between the two hash values, prompts for:

i. Reimage

ii. Ignore

k. Repeat (i) to (iv) till either there is no mismatch or Ignore is selected by the User.

l. Proceed to the next block and repeat (i) to (v) till all the blocks are imaged.

m. Calculate the hash value of the block hash values and hash value of the whole suspect disk (minus the ignored blocks)[31] and the destination disks and authenticate the two, prompting for error and reimaging in case of mismatch.

III. Prompt for following details:

a. Name of the Investigation Officer

b. Rank

c. Date and Time of Seizure and Acquisition

d. Place of scene of seizure and acquisition

e. Crime No.[32]

f. Name of the Police station

g. Custodian of suspect computer

[27] Suspect Computer Environment (SSM a slave), Computer Forensic Workstation or parallel lap link (Suspect Disk- Secondary master, SSM- Secondary Slave)

[28] To make a note in the physical seizure memo.

[29] Primary Master, Secondary Master, Primary Slave, Secondary Slave etc.

[30] Refer note no. 17 supra.

[31] Ignored blocks are discounted for calculating the hash value as otherwise, a mismatch will be there between Suspect and destination drive hash values.

[32] Refers to the FIR No.

h. Name of witness 1 (if done at scene of crime)

i. Name of witness 2[33] (if done at scene of crime)

j. Brief Notes

IV. Extract and Display[34] the following details:

a. Suspect computer's system date and time

b. Suspect computer's configuration

c. Suspect Storage media details

d. Capacity of the drive

e. Amount of data stored on it

f. Hash Value of the whole suspect storage media

g. Hash Value of all the Block Hash values of the suspect storage media

h. Block Size and no. of Blocks

i. No. of ignored Blocks and their starting and ending sector nos.

V. Generate a report consisting of the following:

a. Name of the Investigation Officer

b. Rank

c. Date and Time of Seizure and Acquisition

d. Place of scene of seizure and acquisition

e. Crime No.[35]

f. Name of the Police station

g. Custodian of suspect computer

h. Name of witness 1 (if done at scene of crime) Name of witness 2[36] (if done at scene of crime)

i. Brief Notes Suspect computer's system date and time

j. Suspect computer's configuration

k. Suspect Storage media details

l. Capacity of the drive

m. Amount of data stored on it

n. No. of total Blocks and Block size

o. Starting and ending sector of each block and its hash value

p. No. of blocks ignored and their block nos., starting and ending sector nos.

q. Hash Value of the whole[37] suspect storage media

r. Hash Value of all the Block Hash values of the suspect storage media

s. Calculate the hash value of the generated report

VI. Prompt the IO to remove Trueback and insert SSM Floppy

VII. Transfer the entire report to the CSF floppy along with the hash value of the report, providing for an option to make atleast four copies and more if desired..

Version 2 specifications for Trueback

[33] As per section of Indian Evidence Act, all evidence must be seized in the presence of atleast two, local and independent witnesses.

[34] To enable the Computer Forensic Expert to make a physical note of it.

[35] Refers to the FIR No.

[36] As per section of Indian Evidence Act, all evidence must be seized in the presence of atleast two, local and independent witnesses.

[37] Ignoring the ignored blocks for calculation of total hash value

I. Should provide for a "Preview" option of the storage media in an write block environment, facilitating the investigating officer to seize only those portions which are of relevance to his case.

II. It should be able to acquire the subject media through a crossover network cable. This would be required in cases where disassembling of a computer may be dangerous or, such as in case of laptops, impractical.

III. Trueback should be able to employ standard loss-less compression to create compressed copies of Subject Drives. It should be possible to search, verify and analyse the resulting compressed Evidence Files (Acquired Images) in the same manner as non-Compressed Evidence Files.

IV. It should be possible to place the Trueback Acquired images upon a number of different forms of media, such as external or internal SCSI and IDE hard drives, MO drives, Zip Drives and Jaz Drives. These acquired images should be compressible and achievable to CD-ROM and DVD-R with forensic integrity intact, freeing the previously occupied SSM HDD for other examinations after using DiskScrub utilities.

V. Should be able to acquire data from PDAs, Firewall Devices, RAID sets, including hardware Raids and striped sets.

VI. A utility which allows faster acquisition of IDE drives.

VII. Ability to Seize and Acquire Sparse Evidence Files i.e. user selected portion of the Subject media. The resulting image should contain all the necessary files and folders required to display the full path of the selected file and the file itself. All other portions of the drive should be zeroed out.

User Specification of Analysis Tool

1. Such a tool will be called CyberCheck.
2. CyberChecK shall be contained on a CD ROM as will be used only on a Computer Forensic Workstation.
3. It will be developed in phases, the successive phases adding new features to the tool and being downward compatible.
4. CyberCheck will log[38] the details of the person[39] analysing the evidence, the date and time (as per Computer Forensic Workstation dates and times[40]) at which evidence was loaded and what analysis was made.
5. Analysis tool will mount the acquired image as a read-only file or view the acquired evidence as a 'virtual drive' without ever tampering the acquired image, even when the files are 'undeleted' and viewed. CyberCheck should be able to reconstruct the file structure utilizing the logical data in the bit-stream image. This would obviate the need for restoring the acquired evidence on the Computer Forensic Workstation once again.
6. Throughout the process of analysis, the Analysis Tool will continuously verify the integrity of bit stream image by checking the blocks hash values and prompt a warning whenever such integrity is compromised.
7. CyberCheck will have a Windows type GUI, where expert can move among different views (file, case, volume, gallery etc.) with a click of mouse.
8. it shall a provision of preparing the Trueback bootable disk

Analysis Tool

1. On being loaded, CyberCheck should perform a self-integrity[41] check. Prompt and Exit in case of mismatch in stored hash value and generated hash value.
2. Displays[42] all the storage media connected directly or to the Computer Forensic Workstation in which CyberCheck is running.
3. Displays[43] System Date and Time and prompts for correction, if any.
4. Prompts for either
    a. New case Analysis
    b. Old Case Analysis

5. New case Analysis: Prompts Wizard seeking following details:
    a. Name of Analyzing Officer
    b. Lab Reference Number.
    c. Name and Path of Evidence Folder[44] to be created.
    d. Password
    e. Location and path of the Acquired Evidence[45]

[38] It will be continuous log spread over the entire period of analysis.

[39] The evidence file will be password protected by the Expert.

[40] Should prompt the Expert to correct system dates and times as soon as CyberCheck is loaded.

[41] To ensure that there is no corruption of the tool. This will be done by comparison of the prestored hash value of the CyberChech with the calculated hash value at the time of loading.

[42] So that the Expert verifies that the acquired evidence has been detected by the Workstation and also know its path.

[43] This is necessary because the System date and Time shall be used for generation of log and the Case Report.

[44] Evidence Folder will contain the restored image, the analysis, bookmarks, analysis log and the report.

6. Continuation of Old Case Analysis
    a. Name of Analysis Officer
    b. Password
    c. Name and Path of evidence Folder
7. Essential Features (Phase I)

I. Stitching of blocks in restored image and recreate original seized evidence. It should restore both the physical as well as the logical volumes.

II. Authenticate the Acquired Image during the Analysis by block-by-block hash value comparison as well total hash value comparison. In case of any mismatch, it should bookmark those blocks and put then in another folder called 'Mismatch' in the evidence folder.

III. Map the disk geometry, identify partitions and list the file structure (including OLE[46], NTFS, Windows Registry etc.) and should be able to display the disk configuration. It should be able to reconstruct file systems of forensically acquired DOS, Windows (all variations), Linux, Unix (Sun, Open BSD), CD-ROM and DVD-R file systems.

IV. Special Files

    i. Compound File Analysis: Of such files such as Word Documents, Excel spreadsheets and database files which store internal files and metadata having special evidentiary value. Many of these compound files even have their internal file allocation tables. CyberCheck should allow recovery of such internal files and metadata with the option of mounting those files as a virtual file system to view the structure of internal files and view internal 'slack' and unallocated data.

    ii. CyberCheck should be capable of automatically decompressing and displaying Zip files and their contents for easy investigation of such files. Similarly, e-mail attachment files (Base64, UUE, MIME) should be automatically decoded and searched.

V. Should be able to display all[47] stored and deleted files along with the following details for all files:

    i. File Name
    ii. Short Name (8.3 DOS-convention name)
    iii. File Extension (as entered by the user)
    iv. Deleted date and time (if still present in Recycle Bin)
    v. Last Accessed date
    vi. Last Written Date
    vii. File Created date and time (at that location)
    viii. Entry Modified (for NTFS and LINUX file-system files. It should refer to the pointer for file entry and the information that that pointer contains, such as the size of the file.
    ix. Logical Size
    x. Physical Size
    xi. Starting Extent (starting cluster of the file)

[45] Acquired Evidence could be on a hard Disk, a CD ROM, a Zip Drive etc. Information as displayed in Step r would be helpful.

[46] Relevant in case of Word, Excel, PowerPoint etc. which use OLE file format. OLE files could be storehouse of such useful information as author of file, the creation date, the edit time, the last print date, last revised date, 'last saved by' username, company etc.

[47] Including swap files, file slack, print spool files, files in recycle bin etc

xii. File Type based on Header Information (after signature analysis wrt header information; in case there is any mismatch between file extension and file type, the same should be indicated by a colored icon against that file.

xiii. File Identifier (File Identifier No. stored in Master File Table and allocated to files/ folders in NTFS system)

xiv. Hash Value of file*

xv. Full path of file as stored in evidence file

xvi. Original Path in case of deleted files in the Recycle Bin.

VI. Should be able to sort the above attributes including the four time stamps (File Created, Last Accessed, Last Written, Entry Modified), file names, file signatures and extensions, hash values etc in increasing/ decreasing order of dates and alphabetical order, with sort within sort facility upto two levels.

VII. Should provide a built-in Registry Viewer, which organizes the Windows index.dat file into folders, providing the examiner with an expedient and efficient means to view the Windows registry and determine values. This feature will also allow for easy viewing and recovery of evidentiary data from the slack areas of the registry.

VIII. NTFS Files (Windows NT, XP)

i. Should be able to list out owner, group and permissions organized by owner or group in case of NTFS 4 or NTFS 5 Files. The users and groups should be displayed by their SID (Security Identifier Number).

ii. The compressed NTFS files which are acquired as compressed files by CyberSeize, should be mounted as virtual devices causing the data ti be represented in both compressed and decompressed forms during analysis.

IX. PST Files:

i. Should be able to read PST Files

ii. Extract e-mail for plain text analysis

iii. Should be able to handle both compressible and full encryption

iv. Should be able to ignore passwords.

X. Should be able to extract and make available for view in different colour codes in contextual form (i.e. file slack at the and of file) along with date and time stamps, wherever applicable:

i. Deleted files (should be highlighted by a coloured icon)

ii. Sector slack[48] and cluster slack[49] for every file.

iii. Lost Data[50] and stitch such data with the help of information available from FAT

iv. Unallocated Data

v. Swap Files

vi. Temporary Internet Folder

vii. E-mail Files

viii. Printer Spool Files

XI. Should be able to display

i. Contents of each selected sector in hexadecimal as well as text mode.

* Relevant for Phase II, where it will be used for comparison against the hash values of designated types i.e. Suspect etc.

[48] End of file to end of sector

[49] End of sector to end of cluster.

[50] Data which can not be assigned to any file

ii. Should be able to view compound files such as Registry Files, OLE files, ZIP files, Outlook Express Files, MS Outlook E-mail files, NTFS Compressed files.

iii. Should be able to use an external viewer (such as QuickView Plus) to read any file based on Signature analysis from header.

iv. Should be able to locate, extract, reconstruct and display known graphical image files (including deleted images) in a 'Gallery View' in thumbnail format.

XII. Should be able to support multiple key GREP word search displaying the file and folder in which the key word is located. This search should be performed logically meaning thereby that key word string spanning scattered clusters should result in 'hit', in contrast to physical search.

XIII. Should support book marking Book Marking i.e. exporting specified files and clusters to a separate 'Bookmarks' folder. There should be a facility for the examiner to write 'notes' for each bookmarked entry. CyberChech should build up a table of bookmarked entries in the evidence folder.

XIV. Report Generation: Should give a printout at the end on prompt of all the analysis done in the form of a CyberCheck Report giving out details of:

i. Case FIR No.(depending on evidence loaded)

ii. Acquired Evidence loaded in the case

iii. Description

iv. Total Hash Value

v. Hash value of Generated Report at the time of acquisition

vi. Lab Reference No.

vii. Names of Analysing officers along with relevant dates and times in case analysis was spread over a no. of days.

viii. Name of Evidence Folder

ix. Times and Result of various GREP expressions searches made and search results

x. Bookmarks

xi. Recovered files/ images/ data

xii. Dates and time logs of various searches made

Phase II: Desired Features

I. There should a Preview feature, which allows the examiner to view the subject computer using a standard null-modem parallel (lap-link) cable or through a NIC (Network Interface Card) with TCP/IP. This feature should allow the examiner to view and search all data including deleted files on the target hard drive at once without creating an evidence file and without changing a single bit on the drive. This feature will allow the examiner (or an expert Investigating Officer) to quickly determine whether relevant evidence exists on a computer. It should be possible to conduct text, hash and file signature searches through the preview feature. This would be useful in situation where 'blind' examination of subject media containing privileged documentation is required.

II. It should be possible to perform multiple tasks at the same time, i.e. viewing and sorting files in the foreground when searches, hash analysis etc. are going on in the background. This will save precious time of examiner.

III. CyberCheck should allow:

   i. Addition of multiple acquired media (multiple hard drives, floppies, zip disks, other external media) in the Evidence folder at the same time.

   ii. Search and analyse multiple pieces of subject media at one time.

IV. CyberCheck should provide an integrated Timeline Viewer which allows an examiner ti view all relevant time attributes (File created, entry modified, written, accessed and deleted times) of all the files in the Case (or selected group of files) in a powerful graphical environment. This will enable the examiner to draw connections between various files and their different time stamp data, which is very useful for intrusion response, Internet crimes and computer fraud.

V. Hash Value Library: CyberCheck should support the import and creation of hash-value sets of known system files and should use this to distinguish between system/ utility files and other (suspect) files to narrow down the search. The files so sorted out (system and utility files) should be highlighted by a coloured icon for ease of reference. The search feature should search for hash sets to locate hash values and signatures from files that have been deleted or are otherwise located in unallocated space. It should support adding of new hash values and marking them into categories.

VI. File Signature Library: CyberCheck should maintain a library of known file signatures and corresponding header information so that on file signature analysis, it should be able to display the mismatches. This library should be upgradeable. The search feature should search for file signatures to locate file signatures from files that have been deleted or are otherwise located in unallocated space.

VII. Should be able to analyse data from PDAs and Laptops and RAID sets, including hardware Raids and striped sets.

VIII. Should provide Escript Macro Language support to enable the examiner to build his customised analysis tools such as 'Comprehensive Internet History Report' displaying listing of all accessed URLs and times of access.

IX. The examiner must be able to customise the report generated by CyberCheck.

X. CyberCheck should incorporate the 'Instant Decoding of Non-Text data' including such data in unallocated clusters by selecting the block of data that an examiner wants to view, right clicking on thje mouse and selecting the 'View As' Menu. The options for the 'View As' functions should be: Low ASCII, Hex, 8 bit Integer, 16 Bit Integer, 32 Bit Integer, Windows date/Time, Partition Entry, DOS Directory Entry and Win95 Info File Record. These formats allow the examiner to view the data in a more meaningful way by presenting it in a recognizable format and then allowing him to place the selected data in a bookmark or the CyberCheck Report.

XI. CyberCheck should give full Unicode support in display as well as searches.

XII. Dynamic Disk Support[51]: CyberCheck should automatically detect the disk(s) configuration and should map all the partitions, while still preserving the boot area

[51] Dynamic Disks are hard drives that are upgraded to Dynamic Disks by Microsoft Windows 2000 or XP using Disk Manager. When a disk is made Dynamic, an internal partition handling system is installed on the disk. This system permits the drive(s) to be formatted in several different configurations and several combinations thereof. The partition types are as follows: RAID 0(Striped), RAID 1(Mirror), RAID 5 (Striped with parity), Spanned and Basic.

and unused disk area of each disk for further searching. Systems that do not support Dynamic Disks will only show one partition.

XIII. Ability to encrypt evidence files with a public key for their protection and assign permissions to evidence files.

Research & Development

Project Proposal for Seeking Financial Support

SUMMARY SHEET

1. Title of the Project:

IDENTIFICATION OF APPROPRIATE TECHNOLOGIES & PROCEDURE FOR HANDLING & ANALYSING DIGITAL EVIDENCE

2. Organization
    1. Name: SARDAR VALLBHBHAI PATEL NATIONAL POLICE ACADEMY
    2. Address: SHIVRAMPALLY
       DISTT: RANGAREDDY
       HYDERABAD: ANDHRA PRADESH
    3. Legal Status: GOVERNMENT DEPARTMENT
       MINISTRY OF HOME AFFAIRS – NEW DELHI

3. Chief Investigator
    1. Name ASHOK DOHARE IPS
    2. Designation DEPUTY DIRECTOR
    3. Department Incharge (Research & Senior Courses)
       SVP National Police Academy – Hyderabad
    4.Address Deputy Director (R & SCs)
       SVP National Police Academy _ Hyderabad AP

4. Nature of the Project
   C. Basic Research & Development

5. Objectives of the Project
    1. To make a comparative study of
        a. The various IT Laws Enacted / Proposed in various Countries in the World
        b. The recommended Procedurals Laws with respect to Digital evidence in Various Countries of the World
        c. Identification & Study of various Technologies in use for handling & processing Digital Evidence
    2. And thereafter make recommendations regarding
        a. Legal Lacunas if any in the IT Act 2000, specially with respect to dealing with Computer Related Crimes
        b. Required amendments to the procedural Laws, specially the CrPC
    3. Identification of appropriate Procedures for handling / processing Digital Evidence
    4. Identification / Development of appropriate Technology for handling / processing Digital Evidence.

6. Brief outline of the Project with specific technology fallouts:

The enactment of the Information Technology Act 2000, has posed many a challenges for the police, specially so since it recognizes Digital Evidence as relevant & admissible in Court of law

The Act stipulates various technologies to be used for effective E-commerce & E-governance, but is silent on Procedures & Technologies to be used for

a. Procedures of acquiring & storing of Digital Evidence
b. Procedures & Technology to be used for analysis of Digital evidence
c. Procedures for presenting Digital Evidence in a Court of Law

The Act is silent & does not address to the changes / amendment required in the Procedural Laws of the Country, specially the Criminal Procedure Code (CrPC)

7. Expected outcome in physical Terms
a. Specifications of Subsystem / System

8. Agency with which linkup is Established
Prof Jacob Mathews
Prof R Krishna Murthy
SUPER COMPUTER EDUCATION & RESEARCH CENTRE
INDIAN INSTITUTE OF SCIENCE
BANGALORE – 560012

9. Duration of Project - ONE YEAR

10. Year wise break-up of physical achievements with specific intermediate milestones (in terms of aim & objectives)

End of six months

1. By SVP NPA Team

Completion of :

a. Comparative study of IT Laws in the world
b. IT Act 2000 vis-à-vis other laws
c. Study of the Legal Procedural laws of INDIA
d. Sufficiency of procedural Laws
e. Absolutely necessary amendments required

2. By Combined SVP NPA & IISc Team

a. Identification of identity determination parameters of Digital Evidence storing devices
b. Identification of Data recovery software available
c. Identification of techniques of data recovery

Six month – Tenth month

1. Identification of interface between 1. & 2. above finally leading to identification of

a. Standardised procedures for acquiring / seizing / analysing of digital evidence
b. Recommending the necessary amendments required in the Laws / Codes

Eleventh Month – One year

1. Compilation of a Handbook on the Investigation of Computer Related Crimes

11. Likely end Users

1. Police Departments & all the Other Law Enforcement Agencies
2. Private organizations – for Civil Litigations

12. Name of Organizations jointly participating in the project
    1. SVP National Police Academy
    2. Indian Institute of Science, Bangalore

13. Total Budget

Head	Year	Total
Contribution of SVP NPA		Salary of Investigator Infrastructure Other Facilities
Contribution of MIT		Rs 50,00,000=00 (Rs Fifty Lacs only)
Total		Rs 50,00,000=00 (Rs Fifty Lacs)

Sd/-
Ashok Dohare
(Chief Investigator)
Deputy Director (R & SCs)
SVP NPA
Hyderabad AP

Sd/-
MK SHUKLA
Director
SVP National Police Academy
Hyderabad AP

DETAILS OF THE PROPOSAL
PART 1: BACKGROUND INFORMATION

1. Title of the Project:

IDENTIFICATION OF APPROPRIATE TECHNOLOGIES & PROCEDURE FOR HANDLING & ANALYSISING DIGITAL EVIDENCE

2. Chief Investigator: ASHOK DOHARE IPS Deputy Director SVP NPA
Co- investigator Sh Rakesh Aggarwal IPS Asstt Director

3. Other Investigators of the Project with their designations
From IISc Prof JACOB MATTEWS & his colleagues

4. Brief Biodata Please see enclosures

6. Competence of Investigator in Project Area

Shri Ashok Dohare has presented two papers on allied subjects

1. IT ACT 2000 – Issues & Challenges - During the National level seminar, jointly organized by MIT & CMC in Hyderabad on IT Security in Hyderabad
2. Cyber Crimes – Workshop Organized by CMC in Hyderabad

He is a regular guest faculty in

1. Osmania University – Department of Forensic Science
   a. For Information Technology & Cyber Forensics
2. Railway Staff College – Baroda
3. National Industrial Security Academy

He has been teaching Information Technology ever since, he joined the academy on deputation, in April 2000.

He has conducted many senior level courses on Information Technology for officers of the Police department, with seniority ranging from Additional Director General of Police (officers with about 30 years of seniority) to Supt. of Police.

6. Other Commitments of the Chief Investigator & Co-investigators

The Academy is committed to Research & Development in any field associated with subjects related to Police Sciences (please see enclosures – the Mission Statement of the Academy). The investigators should be able to spend about 50% of their time on the Project. They do not have any responsibilities for any on-going projects; this would be an exclusive project for them till its completion.

7. Details of each of the ongoing / completed projects with the Chief Investigator / Co-investigator / R&D team

The chief Investigator Shri Ashok Dohare has no ongoing projects inhand

He has executed following projects successfully

1. Designing a vehicle mounted refrigeration unit based on Seeback's Effect – in the year 1982 – for partial fulfilment for the award of Bachelors degree in Engineering.
2. Thermal Instabilities in LASER Induced Flows – In the Year 1984 - for partial fulfilment for the award of Masters degree in Mechanical Engineering.

Co-investigator Sh Rakesh Aggarwal was a Golden Jubilee Research Scholar in the Academy, doing Research on Cyber Crimes, for the Year 1999-2000

8. Brief description of other project proposal: NIL

9. Infrastructure and other facilities available

List of major equipments:

i. The Academy is the Premier Police Training Organization of the country. The Academy has the best of the Faculty, handpicked not only to impart the best of the training to the new entrants to the illustrious Indian Police service, but also to its serving alumni – the serving IPS officers.
ii. It houses, a state of art computer network with more than 300 workstations & an connectivity to INTERNET to all the workstations
iii. The Academy has its own Mail server, providing e-mail service to all its Alumni serving any where in the Country

Existing Manpower and other personnel

Being an Academy, the Chief Investigator & Co-investigators would be exclusively devoting their available time for research on the project, however they would have to be provided with additional hands to conduct routine jobs, the expenditure on which has been included in the budget estimates of the project.

10. Expensive Equipments / Facilities available elsewhere which could be made use for the project:

Indian Institute of Sciences Bangalore - Supercomputer Education & Research Centre, is the collaborating agency

11. Details of Collaborating Agency: Indian Institute of Sciences - Bangalore
12. Additional Information if any: NIL

Sd/-
Ashok Dohare
(Chief Investigator)
Deputy Director (R & SCs)
SVP NPA
Hyderabad AP

PART II – TECHNICAL SPECIFICATIONS

1. Aim & scope or the Project:
   1. To make a comparative study of
      i. The various IT Laws Enacted / Proposed in various Countries in the World
      ii. The recommended Procedurals Laws with respect to Digital evidence in Various Countries of the World
      iii. Identification & Study of various Technologies in use for handling & processing Digital Evidence
   2. And thereafter make recommendations regarding
      i. Legal Lacunas if any in the IT Act 2000, specially with respect to dealing with Computer Related Crimes
      ii. Required amendments to the procedural Laws, specially the CrPC
   3. Identification of appropriate Procedures for handling / processing Digital Evidence
   4. Identification / Development of appropriate Technology for handling / processing Digital Evidence

2. Detailed description of the Project
   1. The enactment of IT Act 2000 admits a fact, that the Information Technology Revolution also engulfs our country. The revolution by only routinizing the processes has completely changed the emerging world order. The concept of property has changed. The challenge today is to protect the property, which now is intangible. This is leading to newer and newer types of crimes – computer related crimes. Internet provides worldwide connectivity at the pressing of a button, to both the good people & the criminals. The present day crimes because of this have assumed social dimensions and now it is increasing difficult to trace them to individuals
   2. The enactment of the IT Act is a welcome sign. Now people can store their information in the form of bits & bytes, and this would have the legal status enjoyed by information written and stored on paper. These virtual documents can be exchanged over the Internet and restored in bits & Bytes, the transaction having the same legal status. The Act addresses these two issues of storing data & transactions adequately. It amends the Indian Evidence Act and grants legal recognition to Digital evidence. The Act further amends the Indian Penal Code to incorporate tampering of Digital records in various offences.
   3. The IT Act does not amend the procedural laws of the Country, specially the Criminal Procedure Code. It is generally felt that while handling an absolutely new type of evidence – Digital Evidence, the Old Laws as applicable to the tangible world, cannot be applied ditto. How do we seize a computer? How do we seize a hard disk? What is the procedure for seizing a running (on) computer? The laws need some amendments – which are in tune with the new technology. There is also a need for establishing uniform standards procedures.
   4. Over the years Forensic Science & Medicine had evolved and established it self. The new revolution has given birth to a new science in self – Computer Forensics. The IT Act is also silent on the technologies, which are to be used for reading and recovering deleted data in the computer discs.
   5. In view of the above, research proposal has been submitted. The research project involves a highly technical component. Professors from Supercomputer Education & Research Centre, Indian Institute of Science, Bangalore have kindly consented to participate in the project. The project aim at undertaking a study on the above mentioned issues. The schematics are as follows
   6. Objectives of the Project

a. To make a comparative study of
    i. The various IT Laws Enacted / Proposed in various Countries in the World
    ii. The recommended Procedurals Laws with respect to Digital evidence in Various Countries of the World
    iii. Identification & Study of various Technologies in use for handling & processing Digital Evidence

b. And thereafter make recommendations regarding
    i. Legal Lacunas if any in the IT Act 2000, specially with respect to dealing with Computer Related Crimes
    ii. Required amendments to the procedural Laws, specially the CrPC

c. Identification of appropriate Procedures for handling / processing Digital Evidence
    i. Identification / Development of appropriate Technology for handling / processing Digital Evidence

7. Year wise break-up of physical achievements with specific intermediate milestones (in terms of aim & objectives)

End of six months
1. By SVP NPA Team
Completion of:

- Comparative study of IT Laws in the world
- IT Act 2000 vis-à-vis other laws
- Study of the Legal Procedural laws of INDIA
- Sufficiency of procedural Laws
- Absolutely necessary amendments required

2. By Combined SVP NPA & IISc Team

- Identification of identity determination parameters of Digital Evidence storing devices
- Identification of Data recovery software available
- Identification of techniques of data recovery

Six month – Tenth month

- Identification of interface between 1. & 2. Above finally leading to identification of
- Standardised procedures for acquiring / seizing / analysing of digital evidence
- Recommending the necessary amendments required in the Laws / Codes

Eleventh Month – One year

- Compilation of a Handbook on the Investigation of Computer Related Crimes

3. Need forecast and urgency for the technology:

IT Act having been enacted, it is the responsibility of the Law enforcement agencies now to react and take cognisance of any offence reported. Adequate Laws & legally defendable procedures are required urgently to fight the emerging Computer related Crimes

4. Specific manner in which know-how generated here is envisaged to be translated into production

The research project envisages as an end product

1. Identification / Development of appropriate Technology for handling / processing Digital Evidence.

2. Standardised procedures for acquiring / seizing / analysing of digital evidence
3. Recommending the necessary amendments required in the Laws / Codes
4. Compilation of a Handbook on the Investigation of Computer Related Crimes

The technology / procedures & amendment to the Laws / Code recommended would be submitted for implementation to the Ministry of Information Technology for approval by the appropriate Authority. Once approved the publication of the Handbook on the Investigation of Computer related Crime for general use by the Law Enforcement Agencies of the country would be taken up by the SVP National Police Academy.

5. a) Name of production agencies willing to productionise and market surveys if any made by them regarding demand for the product
b) Alternative production agencies
Not Applicable

6. Period required to complete the project: ONE YEAR

7. Details of work already done by present Investigators/R&D team in this or other areas

a) Successfully completed on schedule : NIL
b) Currently in progress : Nil
c) Abandoned : Nil
d) Industry interaction/know-how transferred : Nil

8. Summary of similar work being done : Not Aware of
elsewhere in the country

9. Information regarding specific intermediate milestones (year-wise)

End of six months

1. By SVP NPA Team

Completion of:

f. Comparative study of IT Laws in the world
g. IT Act 2000 vis-à-vis other laws
h. Study of the Legal Procedural laws of INDIA
i. Sufficiency of procedural Laws
j. Absolutely necessary amendments required

2. By Combined SVP NPA & IISc Team

d. Identification of identity determination parameters of Digital Evidence storing devices
e. Identification of Data recovery software available
f. Identification of techniques of data recovery

Six month – Tenth month

1. Identification of interface between 1. & 2. above finally leading to identification of

c. Standardised procedures for acquiring / seizing / analysing of digital evidence

d. Recommending the necessary amendments required in the Laws / Codes

Eleventh Month – One year

1. Compilation of a Handbook on the Investigation of Computer Related Crimes

10. a) Specific problems, hold-ups and difficulties : Nil
foreseen in the implementation of the project

b) If the answer is not Nil to 10(a), how does :
Chief Investigator propose to overcome them?

11. Detailed PERT/BAR Chart (Separate Sheet) : Please refer to 9 above

12. Details of possible alternative arrangements if the Chief Investigator leaves institution or is unable for any other reason to continue on this project. :

The Chief Investigator is with the Academy on deputation till April 2005. This eventuality shall not arise.

13. Name of other organizations in India or Abroad jointly participating in this effort, Extent of their involvement, specific division Or responsibility, accountability etc.

Supercomputer Education and Research Centre – Indian Institute of Science - Bangalore

14. List the personnel already working in the organization who would be transferred to work full time on this project.

Nil

15. Name of experts whom the Chief Investigator would invite to join the project team as full time/part time member.

Active Cooperation would be sought from Prof Jacob Mathews & his team (from SERC, IISc Bangalore) for the implementation the Research project

Part III - Financial details
Yearly Break-up

The project would be completed in a year, so break-up year-wise is not given

1. Budget Requirements for the Year: Rs 50.00.000.00 (Rs Fifty Lacs Only)

S No	Head	Local	F E	Duty	Total	Borne by Organization	Borne by MIT
1.	Capital equipment	12 lacs	22 lacs	Nil	34 lacs	Invisible since SVP NPA & IISc shall be bearing the cost of infrastructure cost & other non calculable costs	Rs 34 lacs
2.	Consumable stores (SVP NPA)	2 lacs	Nil	Nil	2 lacs	Nil	Rs 2 lacs
3	Manpower (SVP NPA)	5 lacs	Nil	Nil	5 lacs		Rs 5 lacs
4	Travel / Training	2 lacs	2 lacs	Nil	4 lacs	Nil	Rs 4 lacs
5	Contigencies / other expenditures	2 Lacs	Nil	Nil	Nil	Nil	Rs 2 lacs
6	Books & Periodicals	2 Lacs	Nil	Nil	Nil	Nil	Rs 2 lacs
6	Overheads SVP NPA	1 lacs	Nil	Nil	Nil	Nil	Rs 1 lacs
	TOTAL	28 lacs	22 lacs	Nil	50 lac	*****	50 Lakhs

Note: At a latter stage the co-ordinating agency was C-DAC Trivandrum. IISc Bangalore continued to support the project as a consultant and Guide.