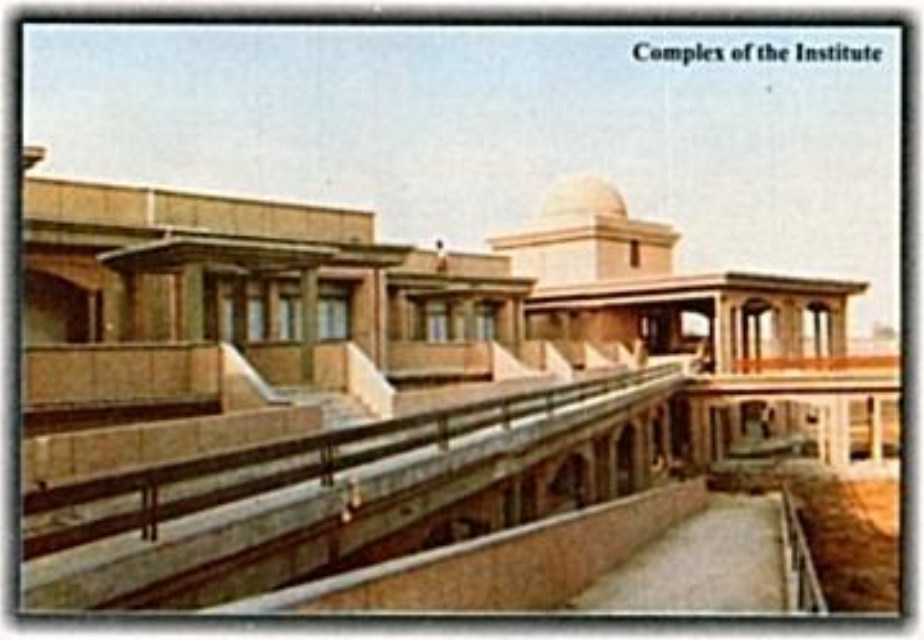
SPECIAL ISSUE ON CYBER LAWS & CRIMES

J.T.R.I.

JOURNAL



INSTITUTE OF JUDICIAL TRAINING & RESEARCH U.P.
Vineet Khand, Gomti Nagar,
Lucknow

Sixth Year
Issue XVI

2001
January

Best Wishes for

Happy New Year

2001

Faculty members :

INSTITUTE OF JUDICIAL TRAINING & RESEARCH U.P.

Vineet Khand, Gomti Nagar,
Lucknow

Prime Minister

MESSAGE

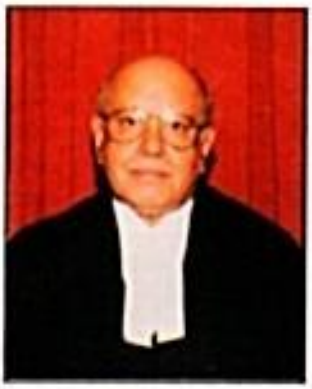
I am happy to learn that the Institute of Judicial Training & Research, Lucknow is organising a national level course on 'Cyber Laws and Cyber Crimes'.

Cyber crimes and cyber laws comprise an area that is new to judicial officers in India. The course being organised by the Institute of Judicial Training & Research will enable judicial officers to better understand the nature and scope of cyber crime and how to deal with them through the application of cyber laws.

I convey my greetings to all participants of this course and my best wishes to the organisers.

New Delhi
November 23, 2000

(A. B. Vajpayee)



Dr. Adarsh Sein Anand
Chief Justice of India

Krishna Menon Marg,
New Delhi-110011

MESSAGE

I am happy to learn that the Institute of Judicial Training and Research is organising a national level Course on ' Cyber Laws and Crimes' in which judicial officers of various High Courts of our country as also judicial officers of Malaysia are taking part. I am also happy to know that Institute is bringing out a special issue of its Journal on this occasion.

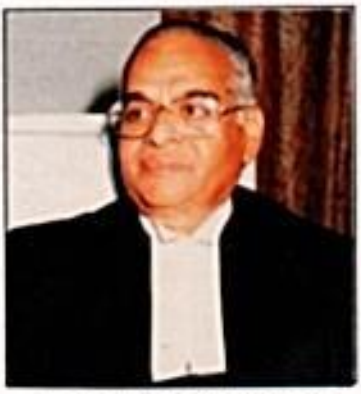
With the passage of time, power and reach of information have changed and created deep anxiety. There is an urgent need to understand the complicated process of changing environment and deliver desired results in the interest of public at large.

I sincerely hope that this course will provide an ample opportunity to the judicial officers to educate themselves with Cyber Laws and Crimes and its implications in the changing society.

I send my good wishes for the success of the Course.

New Delhi
November 20, 2000

(A.S. Anand)
Chief Justice of India



Justice Brijesh Kumar
Judge
Supreme Court of India

New Delhi.
Camp : At Lucknow
December 22, 2000

MESSAGE

I am happy to find that the Institute of Judicial Training and Research, Lucknow, is going to organise a training course on Cyber-laws, Crimes and Intellectual Property Rights for the Judicial officers participating from all over the country as well as some from abroad.

Electronic technology is advancing fast and the age of "electronic commerce" too is arriving with equal speed. Time taking and cumbersome paper transactions may, after some time, get out-dated. Commercial transactions within the country or multi-national in nature may generally be transacted through electronic media. Electronic storage of information and electronic filing of documents would be needed. Such transactions obviously needed legal sanction and consequently the amendments in the existing laws, which only related to paper transactions. Digital signatures and accessibility to communication through computer and its authenticity is very much required and was to be provided for under the law.

This is the right time that at the threshold of the coming era, the Institute has decided to hold this training course to acquaint the officers with such important developments. It is creditable indeed for the Institute.

I hope that the Institute would spread knowledge in this branch of law of "electronic commerce" by holding more such training programmes.

I wish all success to this programme on cyber-laws.

Yours sincerely,

Bkumar

(Brijesh Kumar)

विष्णुकान्त शास्त्री
राज्यपाल, उत्तर प्रदेश

राजभवन,
लखनऊ-227132

संदेश

मुझे यह जानकर अत्यन्त प्रसन्नता हुई कि न्यायिक प्रशिक्षण एवं अनुसंधान संस्थान, लखनऊ द्वारा साईबर लॉज एण्ड क्राइम से सम्बन्धित उच्च विशेषज्ञीय ज्ञान का कार्यक्रम आयोजित किया जा रहा है तथा इस अवसर को अविस्मरणीय बनाने हेतु एक विशेषांक भी प्रकाशित किया जा रहा है।

आज सूचना प्रौद्योगिकी के बिना विकास सम्भव नहीं है। हमारे देशवासियों के जीवन स्तर में संचार तथा क्रियाशीलता समाहित करने के लिए सूचना विज्ञान के प्रसार की अधिक आवश्यकता है। सूचना प्रौद्योगिकी तथा कम्प्यूटर के क्षेत्र में पिछले दशक में हमारे देश में काफी तरक्की हुई है। परन्तु यह तरक्की केवल बड़े शहरों तक ही सीमित रही है, मेरा निश्चित मत है कि सूचना क्रान्ति को गाँव तक ले जाना हमारा लक्ष्य होना चाहिये।

प्रशिक्षण के सफल आयोजन के लिये मेरी हार्दिक शुभकामनाएँ।

(विष्णुकान्त शास्त्री)

High Court
Allahabad
December 18, 2000

MESSAGE

Justice Shyamal Kumar Sen
Chief Justice

I am happy to know that Institute of Judicial Training and Research, Lucknow has arranged a highly specialized national level course on Cyber Law for Judicial Officers of the various States. In recent era, developments in the areas of science and technology particularly information technology and Biotechnology have dramatically changed our civilization. Such developments have unwittingly changed the social structure and values, and in particular the legal system in ways that are beyond our grasp. There is no doubt that information technology and the synchronized progress of other technologies can elevate the quality of life of the people.

Our Judiciary has long been considered inner-performing to the public, and similarly, legal professional often lacks accurate knowledge about the science of the social roles played by both technology and media. This is a time of great change in our justice system. We are seeking more efficient and more affordable ways to provide access to the system, while ensuring that our traditional goals of fairness and impartiality remain inviolate. Technology and demographics are but two forces exerting pressure on our justice system, which must be adopted in creative and innovative ways if we are to retain our place as the model for the world at the beginning of a new century. Such courses would work for professional management, the stream lining of court practices on calendaring and pretrial proceedings and the use of modern technology.

I hope that the Judicial officers who will undergo the training course shall utilize the latest technolgoical advancement in the development of our judicial system.

(Shyamal Kumar Sen)

राजनाथ सिंह

मुख्यमंत्री
उत्तर प्रदेश

सचिवालय एनेक्सी,
लखनऊ
दिनांक 26 दिसम्बर, 2000

संदेश

मुझे यह जानकर अत्यन्त प्रसन्नता है कि इंस्टीट्यूट ऑफ जुडीशियल ट्रेनिंग एण्ड रिसर्च के तत्वावधान में आगमी 6 जनवरी से 18 जनवरी, 2001 तक अन्तर्राष्ट्रीय स्तर का प्रशिक्षण कार्यक्रम CYBER LAWS, CYBER CRIMES AND INTELLECTUAL PROPERTY RIGHTS लखनऊ में आयोजित किया जा रहा है। प्रशिक्षण कार्यक्रम में मलेशिया के न्यायिक अधिकारी भी भाग ले रहे हैं। इस अवसर पर इंस्टीट्यूट द्वारा अपने जर्नल का विशेषांक भी प्रकाशित किया जा रहा है।

विज्ञान और संचार क्रांति के आज के आधुनिक दौर में सूचना प्रौद्योगिकी का महत्व कहीं अधिक बढ़ गया है। कम्प्यूटर और इंटरनेट का इस्तेमाल जनसाधारण के लिए एक जरूरत बन चुका है। ऐसे में इस वैज्ञानिक और तकनीकी रूप से अत्यन्त प्रभावी संचार साधन का दुरुपयोग भी आपराधिक प्रवृत्ति के व्यक्तियों द्वारा अपने स्वार्थों, षड्यंत्रों और गंभीर अपराधों के लिए किये जाने की घटनायें भी दिनोंदिन बढ़ रही हैं। इन अपराधों के नित नये रूप सामने आ रहे हैं। इस परिप्रेक्ष्य में कम्प्यूटर और इंटरनेट से सम्बन्धित कानूनों (साइबर लॉज) को प्रभावी बनाने पर विचार किया जाना अपरिहार्य है। आशा है, प्रशिक्षण कार्यक्रम के दौरान न्यायिक अधिकारी संचार साधनों के दुरूपयोग को रोकने के सम्बन्ध में सार्थक चर्चा कर कोई रास्ता निकालने पर अवश्य विचार करेंगे।

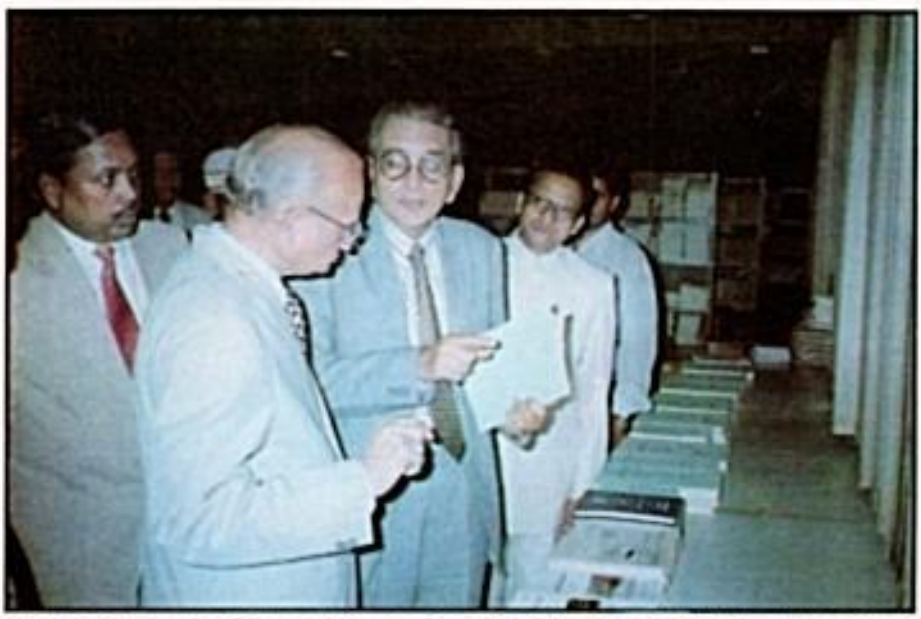
प्रशिक्षण कार्यक्रम और विशेषांक की सफलता हेतु मेरी हार्दिक शुभकामनाएं।

(राजनाथ सिंह)

Hon'ble Mr. Justice Brijesh Kumar, Judge, Supreme Court of India, receiving memento from Sri D.P. Gupta, Director in the Valediction Session of Refresher Training Programme for Additional District & Sessions Judges on 21 Oct., 2000.

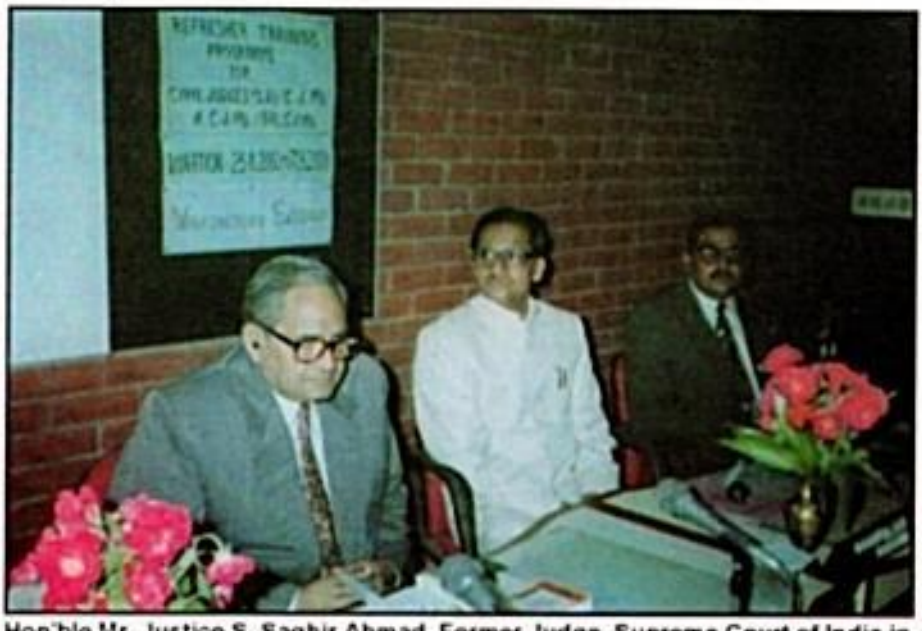
Hon'ble Mr. Justice Brijesh Kumar, Judge, Supreme Court of India, receiving bouquet from Sri D.P. Gupta, Director.

Hon'ble Mr. Justice Shyamal Kumar Sen, Chief Justice of Allahabad High Court addressing Trainees in Refresher Training Programme for Civil Judges (Senior Division) on 28 Aug., 2000. Sri D.P. Gupta, Director, (right) and Sri Nirvikar Gupta, Addl. Director (middle)



Hon'ble Mr. Justice Shyamal Kumar Sen, Chief Justice of Allahabad High Court accompanied by Hon'ble Mr. Justice A.N. Gupta, Chairman, Sri D.P. Gupta, Director and Sri N.V. Gupta, Addl. Director, during His Lordship's visit to Publication Section of I.J.T.R.

Hon'ble Mr. Justice S. Saghir Ahmad, Former Judge, Supreme Court of India (extreme right) and Hon'ble Sri Radhey Shyam Gupta, Law Minister, Govt. of U.P., Hon'ble Mr. Justice Palok Basu, Administrative Judge Lucknow, Hon'ble Mr. Justice A.N. Gupta, Chairman in the inaugural Session of Lucknow Zonal Conference on "Improving Legal and Judicial Governance in U.P." on 23 Sept. 2000.



Hon'ble Mr. Justice S. Saghir Ahmad, Former Judge, Supreme Court of India in the Valedictory Session of Refresher Training Programme for Civil Judges (Senior Division) on 7 Sept. 2000. Sri D.P. Gupta, Director (middle) and Sri A.N. Mittal, Addl. Director (right).

Hon'ble Sri Radhey Shyam Gupta, Law Minister, Govt. of U.P., (middle) being received by Hon'ble Mr. Justice A.N. Gupta, Chairman (right) and Sri D.P. Gupta, Director, (Left) in the Institute on 23 Sept. 2000 for Lucknow Zonal Conference on "Improving Legal and Judicial Governance in U.P."

Hon'ble Mr. Justice Brijesh Kumar, Judge, Supreme Court of India and Hon'ble Mr. Justice G.P. Mathur, Judge, Allahabad High Court interacting with faculty members on 21 Oct. 2000.

Hon'ble Mr. Justice Palok Basu, Administrative Judge, Lucknow receiving bouquet from Sri D.P. Gupta, Director in the inaugural session of Lucknow Zonal Conference on "Improving Legal and Judicial Governance in U.P." on 23 Sept., 2000 seen on dias Hon'ble Mr. Justice S. Saghir Ahmad, Former Judge, Supreme Court of India and Sri N.K. Mehrotra, Principal Secretary, Law. Sri A.N. Mittal, Addl. Director, comparing the programme.

Hon'ble Mr. Justice Palok Basu, Administrative Judge, Lucknow receiving memento from Hon'ble Mr. Justice A.N. Gupta, Chairman in seminar on "Dowry and Dowry Deaths" on 22 July, 2000. Seen in middle Sri D.P. Gupta, Director.

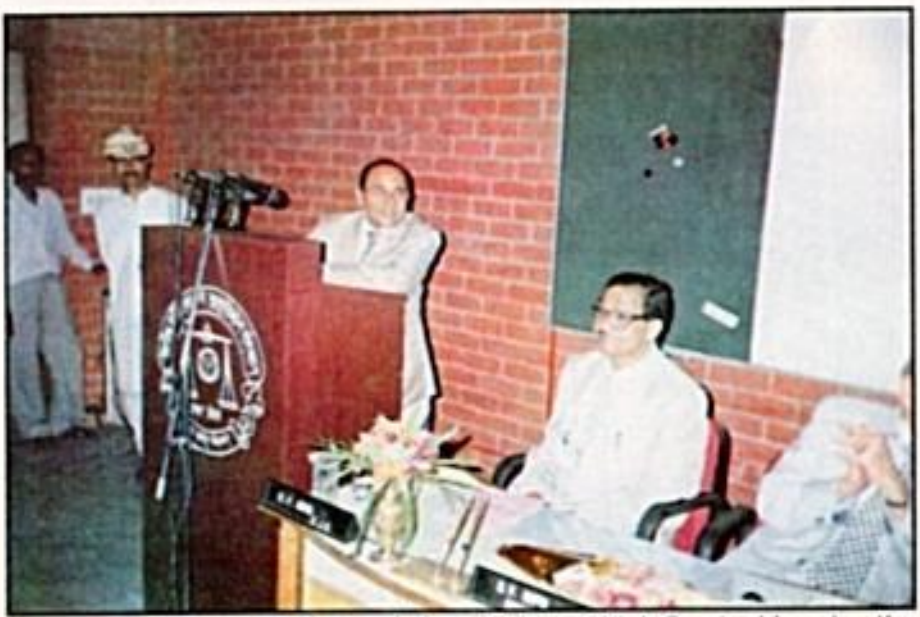
Hon'ble Mr. Justice S. Saghir Ahmad, Former Judge, Supreme Court of India (middle on dias) Hon'ble Sri Radhey Shyam Gupta, Law Minister, Govt. of U.P. and Hon'ble Mr. Justice Palok Basu, Administrative Judge, Lucknow (Left), Sri D.P. Gupta, Director and Sri N.K. Mehrotra, Principal Secretary, Law & L.R. Govt. of U.P. (right) during National Anthem in the Inaugural Session of Lucknow Zonal Conference on "Improving Legal and Judicial Governance in U.P." on 23 Sept. 2000.

Hon'ble Mr. Justice S.H.A. Raza, Senior Judge, Lucknow Bench, Allahabad High Court receiving bouquet from Sri D.P. Gupta, Director in the Valediction Session of conference on "Dowry and Dowry Death" on 22 July, 2000.

Hon'ble Mr. Justice S. Saghir Ahmad, Former Judge, Supreme Court of India, receiving bouquet from Sri D.P. Gupta and Sri A.N. Mittal, Addl. Director Comparing the session.

Hon'ble Mr. Justice S.Saghir Ahmad, Former Judge, Supreme Court of India, addressing the Inaugural Session of Lucknow Zonal Conference on "Improving Legal and Judicial Governance in U.P." seen on the dias Hon'ble Sri Radhey Shyam Gupta, Law Minister, Govt. of U.P. (middle), Hon'ble Mr. Justice Palok Basu, Administrative Judge, Lucknow (Left) and Sri D.P. Gupta, Director (right).

Hon'ble Mr. Justice G.P. Mathur, Judge, Allahabad High Court, receiving bouquet from Sri D.P. Gupta, Director in the Valediction Session of Refresher Training Programme for Additional District & Sessions Judges on 21 Oct. 2000. Seen on the dias Hon'ble Mr. Justice Brijesh Kumar, Judge, Supreme Court of India and Hon'ble Mr. Justice A.N. Gupta, Chairman.

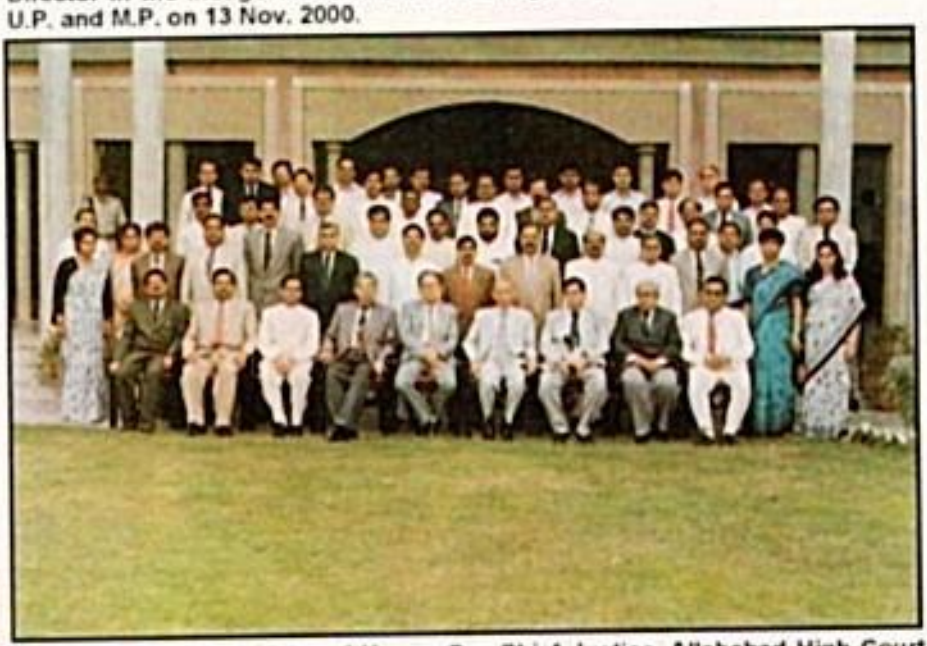


Hon'ble Mr. Justice G.P. Mathur Judge, Allahabad High Court, addressing the Trainees of Refresher Training Programme for Additional District & Sessions Judges seen on dias Sri D.P. Gupta, Director.

Hon'ble Mr. Justice K.N. Goyal, Chairman, State Law Commission, U.P. accepting bouquet from Sri Raghvendra Kumar, Addl. Director in Valediction Session of Seminar on "Dowry and Dowry Deaths" on 22 July 2000. Sri D.P. Gupta, Director (right) and Sri N.V. Gupta, Addl. Director comparing the programme.

Sri V.K. Mittal, I.A.S., Principal Secretary, Home, Govt. of U.P. (middle) alongwith Hon'ble Mr. Justice A.N. Gupta, Chairman and Sri D.P. Gupta, Director (in right) and Sri K.S. Rakhra, D.J., Lucknow and Sri S.V.M. Tripathi, D.G.P. (Retd.) representative NHRC in Seminar on Human Rights on 2 Sept. 2000.

Sri Arvind Mohan, I.A.S., Principal Secretary, Prison, Govt. of U.P. alongwith Hon'ble Mr. Justice A.N. Gupta, Chairman (left) and Sri S.P.S. Pundhir, Addl. D.G., Prison, Sri A.N. Mittal, Addl. Director and Sri Raghvendra Kumar, Addl. Director in the Inaugural Session of Training Programme for Jail Officers of U.P. and M.P. on 13 Nov. 2000.



Hon'ble Mr. Justice Shyamal Kumar Sen,Chief Justice, Allahabad High Court (middle on chair), with (left) Hon'ble Mr. Justice S.H.A. Raza,Senior Judge, Lucknow Bench, Sri D.P. Gupta, Director, Sri N.V. Gupta and Sri A.N. Mittal, Addl. Directors, and (on right) Justice A.N.Gupta, Chairman, Sri N.K.Mehrotra, Principal Secretary, Law & L.R.,Sri P.D. Kaushik, Registrar and Sri J.C.S. Rawat, Registrar in group photograph with Civil Judges (Senior Division) in Refresher Training Programme.

INSTITUTE OF JUDICIAL TRAINING & RESEACH, VINNET KHAND-1, GOMTI NAGAR, LUCKNOW.

FACULTY MEMBERS

PBX No. 300545 E-Mail:jtri_up@satyam.net.in

		Phone Nos.	
		Office	Residence
Hon'ble Mr. Justice A. N. Gupta, Chairman		300547	218969
Sri D. P. Gupta, Director	Fax:	301289 300546	391131 Fax: 392205
Sri N. V. Gupta, Additional Director		300545	210034
Sri A. N. Mittal, Additional Director (Research)		300545	391387
Sri Raghvendra Kumar, Additional Director (Administration)		300545	202087
Sri T. B. Singh, Deputy Director (Administration)		300545	....
Sri Ravindra Maithani, Deputy Director (Research)		300545	302633
Sri R. V. S. Gautam, Deputy Director (Management)		300545	386090
Sri M. M. Ansari, Assistant Director (Accounts)		300545	365301

J.T.R.I. JOURNAL

SIXTH YEAR JANUARY 2001 ISSUE XVI

CONTENTS

Cyber Laws And Intellectual Property Rights

Justice Yatindra Singh
Judge
Allahabad High Court

•

1. New inventions, discoveries and technologies not only widen scientific horizon but also pose new challenges for the legal world. Computers, Internet[1] and Cyberspace[2]- together known

---

• **This is text of talk delivered before faculty members and students of Indian Institute of Technology, Kanpur on 14th October, 2000.**

[1] The District Court for the Eastern District of Pennsylvania in ACLU v. Reno explains the development of the Internet as follows:

> *'The Internet is not a physical or tangible entity, but rather a giant network, which interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks. ...*
> *Some networks are "closed" networks, not linked to other computers or networks. Many networks, however, are connected to other networks, which are in turn connected to other networks in a manner, which permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.*
> *The nature of the Internet is such that it is very difficult, if not impossible, to determine its size at a given moment. It is indisputable, however, that the Internet has experienced extraordinary growth in recent years. ...*
> *No single entity-academic, corporate, governmental, or non profit-administers the Internet. It exists and functions as result of the fact that hundreds of thousands of separate operates of computers and computer networks independently decided to use common date transfer protocols to exchange communications and information with other computers (which in turn exchange communications and information with still other computers). There is no centralised storage location, control point, or communications channel for the Internet, and it would not be technically feasible for a single entity to control all of the information conveyed on the Internet.'*

This case was decided on 11.6.1996. Full text of the judgement is available at : http://www2.epic/org/cda-dc-inion.html).

[2] The Supreme Court of the United States of America (US) in ACLU Vs Reno 521 US 844 explains the nature of Cyberspace as follows:

as Information technology-have also posed new problems in jurisprudence. It has shown inadequacy of law while dealing with the-

(i) information technology itself;
(ii) changes induced by the information technology in the way we live, perceive and do business.

The courts throughout the world have been dealing with these problems and coming up with inconsistent answers. Sometimes these problems have arisen in separate tight compartments mentioned above; some times in combination with each other. These problems have arisen in different areas. These areas are: Intellectual property, electronic commerce or e-commerce (commercial laws), jurisdictional issues, safety concerns, Criminal Law, Evidential issues (i.e. admissibility and relevancy of electronic documents or computer print outs in courts), moral issues and freedom of expression, and privacy protection. The law (statutory or otherwise) providing answers to these problems or dealing with the Information Technology is often loosely referred to as the 'Computer Laws' or 'Information Technology Laws' or 'Cyber Laws'.

INTELLECTUAL PROPERTY

2. *'What is worth copying is prima facie worth protecting.'*[3] This proposition, though laid down about 100 years ago, is truer today for computer software than for any other thing at any

---

'Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorise precisely. But, as presently constituted, those most relevant to this case are electronic mail ("e-mail"), automatic mailing list services ("mail exploders," some times referred to as "listservs"), "newsgroups," "chat rooms", and the "World Wide Web." All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium-known to its users as 'cyberspace'- located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.'

This case was decided on 26th June, 1997 and its full text is also available at:http://www2.epic.org/cda/cd-decision.html).

[3] The portion in italics is from the judgement of Paterson J in University of London vs. University of Tutorial Process Ltd. 1916 (2) Ch 601).

other time. This protection is normally given under Intellectual Property Laws, In India Intellectual Property Laws consist of four different Acts namely Copyright Act, 1957, Design Act, 1911, Patents Act, 1970 and Trade and Merchandise Marks Act, 1958. Let's understand the functioning of computer software before we answer the problems of protecting it.

Object Code

3. Computers do not understand our language. They only understand 'machine language' or 'machine code' i.e. instructions which consist of a series of 0s and 1s. A suitably trained or skilled programmer can write program in machine code for a computer. But the process is slow and tedious and the program, although intelligible to the computer, will be virtually unintelligible to anyone except an equally skilled programmer. From the early days of computers, an alternative language for writing programs was devised. This was known as 'assembler language'. While assembler language had advantages over machine code it still required many instructions to be written in order to achieve the simplest tasks. A number of high- level languages such as Basic Fortran, Cobol, Pascal etc. has been devised in order to simplify the work of the programmer. The use of these high level languages enables the programmer to write a program in terms, which nearly resemble ordinary English than those used in lower level languages. They also permit complex operations for the computer to be directed by a relatively compact command. The programs as written by the programmer are known as the source code. When an assembler or a compiler converts it into machine code, it is known as the object code. This conversion is one way. It is not possible to convert object code into source code.

Source Code, Object Code and Copyright

4. World Intellectual Property Organisation (WIPO) recommended in late 1970 that computer software (object code and subject code) should be protected under the Copyright Acts. The question whether both are so protected or not, has troubled the courts from 1970's and has been answered by the

courts differently. Australian High Court in 1986[4] held that the subject Code is a literary work and is protected as a copyright. But no such protection was given to the object code. The majority held',

> 'I have not found anything .... that has persuaded me that (the object code) a sequence of electrical impulses in a silicon chip not capable itself of communicating anything directly to a human recipient, and designed only to operate a computer, is itself a literary work, or is the translation of a literary work within the Copyright Act.'

Here the law was inadequate to deal with the information technology.

Amendments in the Copyright Act

5. The position in India was similar to that of Australia. It was doubtful if the object code or the computer database was protected under the Intellectual Property Laws in India. The Indian response has been to amend the Copy Right Act by two amending Acts namely Act no. 38 of 1994 with effect from 10th May 1995 and Act no. 49 of 1999 which came into force on 13th January 2000. By these amending Acts some new sub-sections to section 2, namely the interpretation clause, were added and section 2 (o) of the Copyright Act was amended to change the definition of the word 'literary work'. It now includes computer programme as well as computer database. The result is that not only the computer programmes (subject code as well as object code) are protected but computer database is also protected as a copyright. Section 14 of the Copyright Act defines 'copyright'. This section was also amended giving exclusive rights to the owners to do or authorising the doing among the other thing to reproduce, sell, or rent a computer database or a computer programme.

---

[4] Gibbs J. in Computer Edge Pty Ltd vs Apple Computer Inc (1986) 161 CLR 171. Full text is also available in database of judgements of the High Court of Australia at http://www.hcourt.gov.au/)

Remedies for infringement of a Copyright

6. Infringement of a copyright is defined in Section 51 of the Copyright Act. A person infringes a copyright if he, without a license, does an act which only owner has exclusive right to do. Infringing of a copyright not only gives rise to civil remedies but also imposes criminal liability on the offender. Civil remedies are provided under Chapter XII of the Copyright Act and effected person can obtain injunction, damages for the infringement.

7. Penal consequences of an infringement of a copyright are provided in Chapter XIII of the Copyright Act. A person infringing or abetting the infringement is liable to imprisonment, which may extend to three years and fine, which may extend to two lakh rupees (Section 63 of the Copyright Act). There is enhanced penalty for second and subsequent convictions (section 63A of the Copyright Act). Knowingly making use of an infringing copy of computer software on a computer is a separate offence (section 63B of the Copyright Act). It is punishable with imprisonment for not less than 7 days and may extend to three years and with a fine, which shall not be less than 50,000 but may extend to two lakh rupees.

OTHER AREAS

8. Many areas-though not all-where Information Technology had impact have been sought to be remedied by the Information Technology Act (IT Act). I will briefly discuss problems and impact of the IT Act on some of the areas namely e-commerce, jurisdiction issues, security measures, criminal law, Evidential issues and morality qua freedom of expression.

E-COMMERCE

9. A document fulfils many functions but main among them, so far as business is concerned, are two:
   1. It can be used as evidence.
   2. It has symbolic function to show ownership i.e. Railways receipt or bill of lading.

A signed document amongst the others can be used for-

(1) identifying the source of the document
(2) confirming the information;
(3) constituting the proof of signatory's responsibility to the correctness of the information.

10. Information Technology has brought a change. The business is now being done electronically-without use of paper. The advantages of a signed document to a large extent has been sorted out by the information technology by using Electronic Data Interchange (EDI), which is computer-to-computer transmission of business data in a standard format. It is means of business communication where paper is replaced with structured electronic messages and is more secure than e-mail. The signature function is performed by a procedure known as digital signature. The digital signature has two keys, one a private key that is known only to the person concerned and second a public key to check the private key. In this way, a signed message can be sent safely without being tampered. Contracts now can be executed electronically.

11. Some new ways to sort out symbolic function of a document are being proposed though they still have a long way to go. The Comite Maritime International (CMI) recommended rules for Electronic Bills of lading in 1990. Faber in his article 'Electronic Bills of Lading and Functional Equivalence'[5] says, 'The CMI are operated by the carrier issuing to the Shipper and electronic bill of lading using electronic message together with a private code or "key" possession of which entitles the holder to control the goods. This right of control is passed to other interest after notification by the shipper to the carrier who cancels the original key and gives a new key to the new person entitled to control of the goods. In this way the key holder should have right as the bill of lading holder. The CMI Rules are currently a useful set of rules that establish a procedural basis for the use of electronic bills of lading. However, the Rules lack provisions dealing with the issues of what Constitutes an actual receipt of an offer and subsequent

---

[5] 1998 (2) The journal of Information Law and Technology. Full text is available at : http://elj.warwick.ac.uk/jilt.ecomm/98-21iv/livermor.htm)

acceptance. The Rules also have no guideline in the event of system failure."

Soon symbolic functions of a document may also be done electronically.

12. The changes brought about by the information technology while doing business cannot be utilised unless legal recognition is accorded to electronic documents, digital signatures and sufficient security measures are adopted for their correctness. The United Nations Commission on International Trade Law (UNCITRAL) adopted the Model Law on Electronic Commerce in 1996. The General Assembly of United Nations by its Resolution No, 51/162 dated 30th January, 1997 recommended that all States should give favourable considerations to the said Model Law when they enact of revise their laws. The Model Law provides for equal legal treatment of users of electronic communication and paper based communication. The Indian Government has enacted IT Act in response to this resolution. It object and reason state:

> 'New communication systems and digital technology have made dramatic changes in the way we live. A revolution is occurring in the way people transact business. Businesses and consumers are increasingly using computers to create transmit and store information in the electronic form instead of traditional paper document. Information stored in electronic form has many advantages. It is cheaper, easier to store, retrieve and speedier to communicate. Although people are aware of these advantages, they are reluctant to conduct business or conclude any transaction in the electronic form due to lack of appropriate legal framework. The two principal hurdles that stand in the way of facilitating electronic commerce and electronic governance are the requirements as to writing and signature for legal recognition. At present, many legal provisions assume the existence of paper based record documents and records, which should bear signatures. The Law of Evidence is traditionally based upon paper-based records and oral testimony. Since electronic commerce eliminates the need for paper-based

transactions, hence to facilitate e-commerce, the need for legal change has become an urgent necessity. International trade through the medium of e-commerce is growing rapidly in the past few years and many countries have switched over from traditional paper based commerce to e-commerce.

13. The IT Act tries to sort out many problems of the cyberspace. This is done by two ways: firstly by enacting IT Act; secondly by making suitable amendments in the Indian Penal Code 1860, the Indian Evidence Act, 1872 the Banker's Books Evidence Act, 1891, and the Reserve Bank of India Act, 1934. These provisions give legal sanction to digital signatures, electronic records, sort out questions of jurisdiction, evidential issues, security measure, and sanction against obscenity.

14. The IT Act amends Reserves Bank of India Act, 1934 and adds clause (pp) to Section 58. The newly added sub-section empowers the Central Government to frame regulations:

- regulating the fund transfer through electronic means between the banks and other financial institution;
- laying down the conditions subject to which they will participate;
- laying down the manner of such fund transfer;
- providing right and obligations of the participation in such transfer.

Digital Signature –electronic governance.

15. The IT Act gives legal sanction to digital signatures (section 5) and electronic record may be authenticated by means of affixing the digital signature (Sections 3). These sections also provide a procedure. Electronic record is to be converted into another one using 'asymmetric crypto system' and 'hash' function (explained in the IT Act) then incorporating digital signature by the private key unique to that person. Anyone having public key corresponding to the private key can verify this authentication. Chapter III of the IT Act brings about an era of electronic governance. In short this Chapter says that all records where the requirement is to be in writing or in the

typewritten or printed form can now be satisfied if it is made in the electronic form. This chapter also permits publications of the rules and the regulations in the electronic form. The applications and forms may be accepted electronically.

Jurisdictional Issues

16. Chapter IV of the IT Act deals with attribution, acknowledgement and dispatch of electronic Records. They will assist the courts in sorting out problems of jurisdiction in case of breach of contract lest a dispute goes to a court of law.

SECURITY CONCERNS

17. Chapter VI of the IT Act deals appointment of controller and grant of licence to certifying authority who in turn is authorised to issue digital signature certificate. Chapter VII of the IT Act details modalities of issuing Digital Signature Certificate. The Controller is repository of all digital signatures (Section 20). He supervises certifying authorities under the Act and has to lay down standards to be maintained certifying authorities (Section 18). He himself has to maintain standard which are secure from intrusion and misuse (Section 20) Certifying authorities also have to maintain standards, which are secure from intrusion and misused (Section 30).

Deterrent provisions

18. Before discussing deterrent provisions, let's discuss the problems faced by English Courts. One Prestel systems provided free e-mail facilities and access to its database to its subscribers. Gold and Schifreen (accused) were hackers and entered its database by hacking its computer. They were caught and prosecuted in England under the Act under which they could be possibly prosecuted namely Forgery and Counterfeiting Act, 1981. An instrument was necessary to commit the offence under the Act. They were convicted but the court of Appeal (as well as House of Lords) acquitted them. They held that:

- Any instrument for the purposes of this Act had to be similar as other examples in the statutory definition, which were physical objects;

- The electrical impulse in question were only transient, this did not correspond well with the idea of the creation of an instrument;
- The charge was inapplicable due to nature of the offence as the password used was not false, it was genuine, and there was just no entitlement to use it.

The Court of Appeal mentioned;

> 'The conduct [of the accused] amounted in essence to dishonestly gaining access to the relevant Prestel data bank by a trick. This is not a criminal offence. If it is thought desirable to make it so that is a matter for the legislature rather than the courts.[6]

19. Law Commission in England recommended that hacking be made penal. It says;

> 'The main argument in favour of hacking offence does not turn on the protection of information but rather springs from the need to protect the integrity and security of computer system from attacks from unauthorised persons seeking to enter those systems, whatever may be their intention or motive.'

The Commission proposed two offences,

> 'The first a broad offences that seeks to deter the general practice of hacking by imposing penalities of moderate nature on all types of unauthorized access, and the second a narrower but more serious offence, imposes much heavier penalties.'

The IT Act has in principle agreed with it and has tried to achieve this by two ways by providing civil and penal consequences for hacking and other wrongful activities.

Civil Consequences

20. The IT Act prescribes penalty against a person who without permission of the owner access, or downloads, or introduces virus or causes any damage, or disrupts, or denies access to an authorized person to any computer, computer system or

[6] R. vs. Gold (1987) (3) All E R 680 affirmed by House of Lords in 1988 (2) All E R 186.

computer network or charges services to the account of any other person. The penalty is to be paid to person affected. It can extend to one crore rupees (Section 43). The quantification of damage is not left to the civil courts but has been entrusted to an adjudicating officer having experience in the field of Information Technology (Section 46). The guiding factors for quantification of damage is, amount of gain of unfair advantage; amount of loss; and the repetitive nature of the default (Section 47). An appeal lies to the Cyber regulation Appellate Tribunal against the order of the adjudicating officer or of the controller (Section 57). A further appeal lies on question of fact or on law to the High Court (Section 62).

Criminal Law; Penal Liability

21. Criminal liability is dealt in Chapter XI of the IT Act. Tampering with computer source document (Section 65) and Hacking with the computer system (defined in Section 66) are offences punishable with imprisonment which may extend to three years or fine which may extend up to two lakh rupees or both. Securing access to a protected system is punishable with imprisonment, which may extend to ten years (Section 70) The Act also provides penalty for breach of confidentiality and privacy of the information received by a person in pursuance of any of the powers conferred under this Act (Section 72) There is penalty, for publishing false Digital Signature Certificate false (Section 73); and for creating, publishing and otherwise making a digital signature certificate for fraudulent or unlawful purpose (section 74). An offender may be imprisoned for a term, which may extend to two years or fine, which may extend to one lakh rupees. Computers, floppies, compact disks or others accessories in respect of which the IT Act or the Rules or the orders thereunder have been contravened are liable to be confiscated. The punishment and confiscation under the IT Act does not interfere with any other punishment to which a person may be liable (say punishment under Copyright Act or the punishment under Indian Penal Code).

Extra Territorial Application

22. The Act has extra territorial jurisdiction. Hackers or persons causing damage to the computers, computer system or computer network located in India are also liable to be punished irrespective of their nationality or place of committing offence (Section 75).

23. The IT Act also amends Indian Penal Code. The word document now includes in electronic record. The result is that anyone using the forged electronic record is punishable under the Indian Penal Code, as he would be of using a forged document.

24. Neither any law can be enacted for all problems can be perceived. Whether there are sufficient security measures to prevent the story of the movie 'The Net' becoming a reality is for the future to disclose.

EVIDENTIAL ISSUES: ADMISSIBILITY IN COURT PROCEEDINGS

25. Is a Computer Printout admissible in a court of law? Let's see what English courts have done on this score. One Pettigrew[7] was accused for committing burglary and for handling stolen goods. He was also found with new notes that had come from a bundle of notes, which were stolen. The prosecution produced a computer print out from the bank of England, which tended to prove that bank note found in the accused possession came from the bundle, which was stolen in the burglary with which the accused was charged. The court of appeal did not admit these computer printouts on the ground that no witness could claim first hand knowledge of the various contents and they must be hearsay. The accused was set free.[8]

26. The IT Act takes care of such situation. It makes necessary amendments in the Indian Evidence Act, 1872, and the

---

[7] R v. Pettigrew (1980) 71 Cr. A R. 39.

[8] The other case in Myers vs. Director of Public Prosecutions 1964 (2) All ER 881=(1965) 1 AC 1001 (HL). In this case the records were kept on the card index rather than on a computer (as would doubtless be the case today). These records were rejected on the principle of hearsay and accused was set free.

Banker's Books Evidence Act, 1891. These amendments have been made in order that electronic record, digital signature and the computer printout may be proved and admitted in court of law. Of course, this can be done only if conditions mentioned in the amended sections are satisfied.

MORALITY: FREEDOM OF EXPRESSION

27. It is often said that if your child is spending too much time alone on a computer then one should be careful. The reason is that the content in the cyberspace is as diverse as human thought. It also contains information and material, which is obscene. An impressionable one can be misled or lured by others. The US in order to curtail it enacted the Communications Decency Act of 1996 (CDA). Section 223 (a) (1) (B) (ii) of the CDA criminalized the 'knowing' transmission of 'obscene or indecent' messages to any recipient less than 18 years of age. Section 223 (d) prohibited the 'knowing' sending or displaying to a person less than 18 of any message 'that', in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs'. Under the CDA it was valid defence, for whose who-

    a. Took in 'good faith, ...effective ..... actions' to restrict access by minors to the prohibited communications (section 223 (e) (5) of the CDA) and
    b. restricted such access by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number {section 223 (e) (5) (B) of the CDA}.

28. The previously mentioned provisions of the CDA Act were challenged in the US. They were struck down by the District Court of Pennsylvania [9] holding:

> 'True it is that many find some of the speech on the Internet to be offensive and amid the din of cyberspace many hear discordant voices that they regard as indecent. The absence of governmental regulation of Internet contents has unquestionably produced a kind of

[9] ACLU vs. Reno (Para 3 of this Acticle)

chaos, but .... what achieved success was the very chaos that the Internet is. The strength of the Internet is that chaos.'

The US Supreme Court affirmed this.[10]

29. The US Government enacted another law known as the Child Online Protection Act (COPA) after the CDA was struck down. COPA is US government's second attempt to regulate the dissemination of indecent material to the minors on the Web/Internet. Under this Act, Commercial Web publishers are to ensure that minors do not access the harmful material on their Web site. COPA was also challenged in the US courts in ACLU vs Reno II.[11] The District Court as well as US Court of appeal for third circuit have granted preliminary injunction preventing COPA's enforcement because the court was confident that the ACLU's attack on COPA's constitutionality is likely to succeed on the merits.

30. The IT Act also tries to balance moral issues with freedom of expression. Publishing or transmitting obscene information in electronic forms is punishable and a person guilty is liable to be imprisoned which may extend to 5 years or fine, which may extend to one lakh rupees. This could be enhanced to ten years or rupees two lakh in case of second or subsequent conviction. The US Courts have invalidated some provisions of their Acts because of the first amendment to the US constitution that provides unqualified right of freedom of expression but Indian Constitution permits reasonable restriction {(Article 19 (2) of the Constitution)}. However, what the Indian Courts will do is to be seen.

GREY AREAS

Right of Privacy

31. The right of privacy is part of Article 21 but it is not absolute. Disclosure of private information is justified under certain circumstances.[12] Nevertheless, right of privacy in the light of

---

[10] ACLU vs. Reno 521 US 844 (Para 4 of this Article) at Page 26.

[11] Full text of the judgement dated 22.6.2000 is available at : http://www.epic.org/free-speech/copa/ed-cir-opinion.html.

[12] X vs. Hospital Z (1998) 8 SCC 296.

Information Technology may have to be dealt by the Courts or suitable legislation may have to be enacted. The right of privacy may be infringed by:

(i) utilising private data already collected for a purpose other than for which it was collected;
(ii) sending of unsolicited emails or spamming;
(iii) unauthorised reading of emails of others.

32. Computer data often contain personal information. It is automatically collected. This is done for use for a particular purpose but this data may be used for any other purpose. This may affect the right of privacy of an individual. Such information is automatically collected where sales are through credit cards; perhaps in future all where sales will be through credit card. This may breach with private rights of individuals who may like to keep his personal history with themselves. England had enacted Data Protection Act to solve this problem.

33. Unsolicited emails are a menace. They should have provision to unsubscribe them or they may not be sent unless asked for. Many states in the US[13] have enacted laws against unsolicited mails known as spam laws. Perhaps with usage of e-commerce we might need similar laws.

Intellectual Property

34. The question regarding trademark in cyberspace will be repeatedly raised with increase of e-commerce. The problem with trademarks on the Internet often is whether trademark use has occurred. In the 'real' world, one can put a label on a product or put a sign on a building, but in the on-line context the use of the trademark may be as ephemeral as a momentary appearance on a computer screen.. Is this enough? A similar issue exists on the infringement front. If some one copies a trademark on to an electronic bulletin board, is this an act of infringement or unfair competition.

[13] A detail summary of these laws is available at http://spamlaws.com.

35. The other grey area in intellectual property is regarding domain name disputes. To exist on the Internet, one must have an address, called a 'domain name'. Different suffixes denote different entities. The '.com' suffix denotes commercial entities. Other suffixes in use are '.org' for non-profit organizations, '.edu' for associations, '.gov' for government. Is use of a domain name that is popular name of other illegal? The probabilities are that domain names are protected under relevant Intellectual Property Laws but the law will become clearer as the courts decide cases.

The Napster Case

36. Shawn Fanning (high school nickname Napster-a refrenece to his nappy hair) wanted to share his music in the computer with his friends. He thought of developing software so that music in one computer could be exchanged with another. No other person thought it to be a good idea. He, still in his teens, left his college to create software combining UNIX server and window operating system so that music in MP 3 format may be transferred. In order to do it, one has to download Napster (provided free of cost on registration) and install it in the computer. This enables the computer to log on to the Napster server. When a request is made, the Napster server searches other users online who may have that music file. If there is one then Napster puts both computers directly in touch with each other so that music files can be downloaded. The Napster server merely puts computers directly in touch with each other but the copyrighted music does not go through its server i.e. it does not receive or contain illegal music at anytime. It merely permits transfer of music files (MP 3 format) from one PC-or peer-to another (P2P). At present that there are about 25 million Napster users. The result is that one can download music files, which may be copyright of others free of cost.

37. Several record companies filed a suit against Napster restraining it from engaging in or assisting others in copying, downloading, uploading, transmitting or distributing copyrighted music without the express permission of its rightful owner. According to Napster it is merely a space-shift

similar to time-shift in the Sony Corporation case[14] and it seeks expansion of 'fair use' doctrine articulated in that case. The District Court of Northern district of California (Judge Marilyn Hall Patel) has granted a preliminary injunction against Napster from engaging or facilitating for copying, downloading, transmitting or distributing plaintiffs' copyrighted musical compositions.[15] Though the appellate court has stayed the preliminary injunction granted by the District Court.

38. The final decision in this case may have serious implications not only in the field of music but also in all other areas of intellectual property rights. In case there is any need then Napster may be easily banned as it has an office and everyone wishing to download a file has to go through the Napster server. But this may be difficult in case of newer software 'Gnutella' which is still in development stage. It neither has any office, not any server. One merely has to install it on a computer and send a message to another computer online that in turn forwards it to other computers online. This goes on till one finds a computer that has required file. Then Gnutella directly connects these two computers and file can be downloaded. It is decentralised and not restricted to MP3 format: it works on all kinds of files. The other similar software 'Freenet' is also in the pipeline. It would be difficult to ban it as:

---

[14] Sony Corporation had made VCRs that could record TV programmes. This has changed the way we watch TV. One can, with the help of a VCR, record programmes, which may be copyrights of others and see it at the later time. owners of copyrights on television programme sued Sony Corporation alleging that :

- Individuals have used the VCRs to record some of the owners' copyrighted works on the TV.
- These individuals had infringed the copyrights and
- Sony Corporation was liable for such infringement because of their sale of the VCRs.

The US Supreme Court dismissed the suit and in Sony Corporation vs. Universal City Studios 464 US 417 held that:

- The time shift for watching the TV programme for private viewing was fair use and it does not infringe copyright.
- A manufacturer is not liable for selling a staple article of commerce that is capable of commercially significant non-infringing uses.

[15] Full text of judgement is available at http://news.cnet.com/news/Pages/Special/Napster/napster-patel.html.

- there isn't any central server,
- it is decentralised, and
- Gnutella files looks like ordinary web traffic.

If file sharing over the Internet is illegal then trying to stop it may be difficult. New concepts or new strategy may have to be thought about.

CONCLUSION

Last year Michael Lewis wrote a book on success story of the Silicon Valley entitled 'The new new thing: a Silicon Valley story'. The most quoted line from this book is, '*The definitive smell inside a Silicon Valley start-up was of curry.*' Let's hope that-with better understanding of cyber problems, their solutions, and cyber laws-not only inside a Silicon Valley start up but also the operating system of e-commerce and cyberspace will smell of curry and I repeat Indian

*****

"I have not a shadow of a doubt that any man or woman can achieve what I have, if he or she would make the same effort and cultivate the same hope and faith. What is faith if it is not translated into action?"

-Mahatma Gandhi

RESOLVING DOMAIN DISPUTES UNDER THE ICANN UNIFORM DISPUTE RESOLUTION POLICY

Chetan Nagendra [1]

The Internet is a worldwide system of computer networks - a network of networks to which any user can connect, using a computer. The beauty of the Internet is that it relies on an underlying centralized hierarchy built into the domain name system (DNS) to control the routing for the vast majority of Internet traffic.

The DNS is the way of locating domain names[2] and translating them into Internet Protocol addresses. A domain name is a meaningful and easy-to-remember 'name' for an Internet address.[3] Second-level domain names must be unique on the Internet and registered with an accredited registrar for the Generic Top Level Domains (.com, .net and .org) and the geographic country code top-level domains. At its heart

[1]* Case Western Reserve University, Cleveland, Ohio, USA. E-mail: chetan@pobox.com

[2] A domain name locates an organization or other entity on the Internet. For example, the domain name www.timesofindia.com locates an Internet address for "timesofindia.com" at Internet point 216.136.134.135 and a particular host server named "www". The "com" part of the domain name reflects the purpose of the organization or entity (in this example, "commercial") and is called the top-level domain name (TLD). The first part, "timesofindia" reflects the organization and together with the top-level is called the second-level domain name. The second-level domain name maps to and can be thought of as the "readable" version of the Internet address. On the Web, the domain name is that part of the Uniform Resource Locator or URL that tells a domain name server using the DNS (domain name system) whether and where to forward a request for a Web page. The domain name is mapped to an IP address (which represents a physical point on the Internet). The domain name system contains an even higher level of domain than the top-level domain. The highest level is the root domain, which would be represented by a single dot. If the dot for the root domain were shown in the URL, it would be to the right of the top-level domain name. However, the dot is assumed to be there, and is never displayed. See generally, http://lookup.atomica.com/atomica/.

[3] For a more detailed definition see, http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,213908,00.html

is a single data file, known as the 'root.'[4] Control of the root provides singular power in cyber-space.[5]

THE HISTORY OF ICANN

The Internet Corporation for Assigned Names and Numbers (ICANN) is a private, non-profit corporation, with responsibility for Internet address space allocation, protocol parameter assignment, domain name system management, and root server system management functions, the service previously performed by the Internet Assigned Numbers Authority (IANA). The late Dr. Jonathon Postel, who headed IANA, chose initial members of the ICANN board. IANA derived its authority under a contract from the U.S. government, which financed the original research network, ARPANET, from which the Internet grew. The need to internationalize the governing of the Internet led the U.S. government to recommend the origin of ICANN as a global, government-independent entity to manage the systems and protocols that keep the Internet going. The U.S. government is essentially turning over control of the Internet to ICANN although domain name registration performed by Network Solutions, Inc. will continue to be under U.S. government contract for a limited time. ICANN has a board of nineteen Directors, nine Directors, nine to be nominated by Supporting Organizations, and the President/CEO (ex officio).

THE UNIFORM DISPUTE RESOLUTION POLICY

Among other activities, ICANN adopted the Uniform Dispute Resolution Policy (UDRP)[6] in October 24th, 1999 for the resolution of Domain disputes in the Internet realm. The principal aim of the UDRP

---

[4] On the Internet, the root server system is the way that an authoritative master list of all top-level domain names (such as .com, .net, .org, and individual country codes) is maintained and made available. The system consists of 13 file servers. The central or "A" server is operated by Network Solutions, Inc., the company that currently manages domain name registration, and the master list of top-level domain (TLD) names is kept on the A server. On a daily basis, this list is replicated to 12 other geographically dispersed file servers that are maintained by an assortment of agencies. The Internet routing system uses the nearest root server list to update routing tables.

[5] A. Michael Froomkin, *Wrong Turn in Cyberspace: Using ICANN to route around the APA and the Constitution*, available at http://www.law.miami.edu/~froomkin/articles/icann1.pdf.

[6] The UDRP is available online at http://www.icann.org/udrp/udrp.htm.

is to be an effective tool against cyber squatters. ICANN jurisdiction is all pervasive and covers

The UDRP provides a framework for the resolution of disputes over the abusive registration of a domain name and covers:

1. Any .com, .net and .org domain names

2. Country code top-level domain names provided that the relevant domain name registration agreement incorporates the UDRP.

DISPUTE RESOLUTION SERVICE PROVIDERS

ICANN has approved four dispute resolution providers to implement the UDRP. They are the World Intellectual Property Organization (WIPO), the National Arbitration Forum (NAF), eResolution (DeC), and the CPR Institute. Dispute Resolution Service Providers typically decide the outcome of most cases two factors listed in UDRP Para. 4(a)(ii) & (iii)(i) the ability of the complainant to show that the respondent has no rights or legitimate interests in the domain name, and (ii) that the respondent has shown bad faith in registering and using the domain name. For domain name disputes involving domain name brokers, the principal deciding factors are usually the nature of the domain name and the strength of the trade or service mark held by the complainant.

The UDRP also gives the approved dispute-resolution service providers limited jurisdiction to hear and decide cases involving 'abusive registrations'. Abusive registrations are those made with bad faith intent to profit commercially for existing trademarks.

DISPUTE RESOLUTION PROCEDURES

A complainant under the UDRP must assert and prove that:

1. The respondent's domain name is "identical or confusingly similar to a trademark or service mark in which the complainant has rights"

2. The respondent has "no rights or legitimate interests in respect of the domain name"

3. Respondent has shown bad faith in his registration and use of the domain name.[7]

Paragraph 4(b) of the UDRP provides non-exclusive guidelines for proving registration and use in bad faith. Similarly, Paragraph 4(c) sets forth three non-exclusive circumstances that demonstrate a registrant's rights to and legitimate interests in a domain name. The provisions in Paragraphs 4(a)-(c) are designed to inform all substantive decisions during the administrative proceeding.

What is unusual in the UDRP is that it requires the complainant to prove all the elements mentioned above and either of these requirements not being fulfilled may result in a complaint being denied. Therefore, the first requirement is that the domain name must be identical to or confusingly similar to a trade name or service mark that the complainant has rights in. Secondly, the complainant must show that the respondent has no rights or legitimate interests in the domain name, and that the respondent has shown bad faith in registering and using the domain name to succeed in his complaint.

TRENDS IN RESOLVING DOMAIN DISPUTES UNDER THE UDRP- A HARBINGER FOR A TOUGHER INTELLECTUAL PROPERTY REGIME

Several interesting cases have come up before the Dispute Resolution Providers under the UDRP within the United States. In *World Wrestling Federation Entertainment, Inc. v. Michael Bosman*[8] the dispute resolution panel held that *"the desire to resell*

[7] ICANN Uniform Domain Name Dispute Resolution Policy Paragraph 4(a).

[8] WIPO Case D99-0001 (decided January 14, 2000).

the domain name is sufficient to meet the 'commercial use' requirement of the Lanham Act."[10]

> While this holding speaks to whether or not there is use, it does not address the question of good or bad faith. Paragraph 4(b)(i) of the UDRP grants that the registration for the primary purpose of selling, renting or otherwise transferring the domain name to the trademark owner is evidence of bad faith. It seems unnecessary, and maybe even impossible, for one to act in bad faith if there is a right or legitimate interest. The reverse is also true: it is just as difficult or impossible to find a legitimate interest if bad faith is shown in the registration and use. These are not absolute statements, but they reflect the general trends demonstrated in the proceedings and decisions to date that may lend some predictability and uniformity to this mandatory process.[11]

Most disputes under the UDRP are influenced by early decisions of the US Courts in Intermatic v. Toeppen and Panavision Intl' v. Toeppen. Both cases have shed some light on the novel legal issues presented where a domain name is used to identify a Web site not tied to any particular goods or services, or where nothing is posted on the Web site.

THE 'COMMERCIAL USE IN COMMERCE' DOCTRINE

Dennis Toeppen, the defendant in both cases, operates an Internet service provider business in Illinois. He registered approximately 240 Internet domain names, many incorporating well-known trademarks such as "deltaairlines.com," "britishairways.com,"

---

[9] The commercial-use requirement is routinely satisfied when a defendant offers goods or services in connection with the offending mark--the typical scenario in most dilution and infringement cases.

[10] The Lanham Act defines the statutory and common law boundaries to trademarks and service marks. Rights to use a trademark are defined by the class for which the trademark is used. Therefore, it is possible for different parties to use the same trademark in different classes. The Lanham Act defines the scope of a trademark, the process by which a federal registration can be obtained from the Patent and Trademark Office for a trademark, and penalties for trademark infringement.

[11] See generally, Cynthia-Clair Tagoe, *Internet Domain Disputes Under ICANN's Uniform Dispute Resolution Policy*, The Internet Law Journal, available at http://www.tilj.com/content/intellectualpeoperty.htm.

"neiman-marcus.com," "crateandbarrel.com," "ramadainn.com," "ussteel.com," "eddiebauer.com," "australianopen.com," and "yankeestadium.com." Toeppen registered these domain names hoping to sell them to the trademark owners.

In *Intermatic, Inc. v. Toeppen*,[12] Intermatic, a well-known manufacturer of a variety of electronic products under the mark 'Intermatic,' sought to enjoin Toeppen from using and registering the domain name "intermatic.com."

In Panavision Int'l. v. Toeppen, plaintiff Panavision, owner of the marks 'Panavision' and 'Panaflex,' well known for its theatrical motion picture and television camera and photographic equipment business, sought to enjoin Toeppen from using and registering the domain names "panavision.com" and "panaflex.com."[13]

The Courts ultimately applied the US Federal Trademark Dilution provision of the Lanham Act, known as the Federal Trademark Dilution Act. This Act requires that a defendant's diluting use of a trademark be a "commercial use in commerce" to be actionable. In both cases, Toeppen argued that his registration and use of the domain names did not satisfy the "commercial use in commerce" requirement of the Dilution Act because none of the sites was tied to any specific goods or services. But in both cases, the courts disagreed.

The Intermatic court rejected the argument that the use of the domain name was commercial merely because it was registered in the ".com" or "commercial" class of domain names. The court reasoned that under NSI's domain-name registration parameters, the ".com" designation is available for both commercial and private use, such that use of a ".com" domain name could be entirely noncommercial. Instead, the Intermatic court ultimately found Toeppen's use "commercial" because of his intent to sell the "intermatic.com" domain.

---

[12] 40 U.S.P.Q.2d 1412 (N.D. Ill. 1996)

[13] 945 F. Supp. 1296 (C.D. Cal. 1996).

Interestingly in Panavision, the court held that the registration of a trademark as a commercial domain name does not by itself satisfy the "commercial use" requirement of the Lanham Act, but found that Toeppen's registration of domain names intending to sell them for profit constituted a "commercial use in commerce." The court also weighed against Toeppen his "business" plan of selling other domain names to the owners of the trademarks incorporated in the domain names.[14]

THE 'LIKELIHOOD OF CONFUSION' DOCTRINE

Another important issue that arises in domain name infringement cases is whether the mere registration of the domain name is a cause for likelihood of confusion necessary to establish trademark infringement.

In the Intermatic case, the court examined whether Toeppen's use of "intermatic.com" was likely to cause confusion by leading consumers to believe that Intermatic sponsored or otherwise authorized Toeppen's activity, the test for trademark infringement. The court looked to the factors commonly employed to determine whether a likelihood of confusion exists. Eventually, the Court decided the case based on the strong trademark enjoyed by Intermatic and Toeppen's use incorporating the entirety of Intermatic's mark, adding only the designation ". com" was not enough for Toeppen to continue using the former's mark. Although there was no evidence to show that Toeppen intended to pass off any goods or services as Intermatic's, especially when no goods or services were offered, a question of fact existed as

---

[14] Commenting on the Court's decision in both cases, David M. Kelly and Douglas A. Rettew, *Courts Order Internet "Pirate" to Walk the Plank*, available at http://www.finnegan.com/pubs/internet/internetpirate.htm. comment- "[...] under Intermatic and Panavision, registration of a domain name incorporating another's mark satisfies the "commercial use" requirement of the Lanham Act if the registrant registered the domain name with the intent of selling it back to its rightful owner. As a matter of proof, however, many defendants may not admit to such a motive, as was the case in Intermatic. Further, not all defendants will have registered over 200 domain names incorporating the marks of others, as was the case in both Intermatic and Panavision. Thus, it is important that a plaintiff produce evidence showing that the defendant registered the domain name with the intent to arbitrage it. The best example, of course, would be any proof that the defendant approached the trademark owner with an offer to sell the domain name or made such an offer in response to the trademark owner's demand that the defendant relinquish the domain name."

to whether his registration of a number of other domain names evidenced his intent to trade on the goodwill of Intermatic.

THE 'DILUTION OF TRADEMARKS' DOCTRINE

Dilution, under the US Lanham Act typically encompasses two types of activity: "blurring" and "tarnishment." Blurring refers to unauthorized uses of a mark with unrelated goods or services that dilute the mark's distinctiveness. Tarnishment refers to unauthorized uses of a mark with unwholesome or shoddy goods or services that tarnish or degrade the mark.

Coming back to the Intermatic case, the court found that Toeppen's registration of "intermatic.com" diluted Intermatic's mark in two ways. First, relying on the statutory definition of dilution as "lessening of the capacity of a famous mark to identify goods or services," the court held that Toeppen's registration of "intermatic.com" lessened Intermatic's ability to identify and distinguish its goods and services on the Internet. Therefore, Toeppen's registration of "intermatic.com" precluded Intermatic from identifying its goods and services on the Internet under the "intermatic.com" domain name. Secondly, the US Court held that Toeppen's use of the "intermatic.com" domain on his Web site diluted Intermatic's rights because it lessened Intermatic's ability to control the reputation and association the public makes with its mark. Specifically, the court found that if Toeppen were allowed to use the "intermatic.com" domain name, "Intermatic's name and reputation could be at Toeppen's mercy and could be associated with an unimaginable amount of messages on Toeppen's web page."

In the Panavision case, the court supported the dilution doctrine based upon Panavision's inability to identify its products on the Internet under the "Panavision" and "Panaflex" names vis-à-vis Toeppen's use of the domain name in the latter's web page. Acknowledging that Toeppen's conduct varied from the standard dilution theories, the court stated that by eliminating Panavision's ability to use its marks "in a new and important business medium," Toeppen's activity diluted Panavision's marks.

AN ANALYSIS OF THE 'RIGHTS OR LEGITIMATE INTERESTS' AND 'BAD FAITH REGISTRATION AND USE' RULES UNDER THE UDRP

Under the UDRP Para. 4(c)(i), domain name registrants must show that they have rights to or legitimate interests in a domain name by proving that even before they had any knowledge of the dispute, they were using or preparing to use the domain name in connection with a bona fide offering of goods or services.

Also, under UDRP Para 4(c)(ii)-(iii) if the respondent can prove that he has been commonly known by that domain name or that he is making a legitimate non-commercial or fair use of the domain name, it would suffice to show a right to or a legitimate interest in the domain name.

Several cases have been decided from the above regulations. In *20th Century Fox Film Corp. v. Risser,*[15] the registrant contested that he registered the domain name 'foxnetworknews.com' (among other domain names that include the word "fox"), to use for his proposed website design business. The dispute resolution panel rejected this as proof of legitimate interest since the proposed use had no rational relationship to the registered domain names.

In *Boardwalk Bank v. Thorogood,*[16] the respondent had registered about 75 domain names, including boardwalkbank.com, but had not used any of them in anyway. Thorogood, the respondent, insisted that he had legitimate interests in the domain name in suit because he had "many, many marketing ideas" but that he had not yet determined the best course of action for the domain name in dispute. The panel rejected this argument as not demonstrating any right or legitimate interest in the domain name vis-à-vis the complainant.

In *Draw-Tite, Inc. v. Plattsburgh Spring, Inc.,*[17] the respondent produced invoices of sales as evidence of use of the domain name

---

[15] NAF Case FA0093761 (decided Feb 15, 2000).

[16] WIPO Case D2000-0213 (decided May 20, 2000).

[17] WIPO Case D2000-0017 (decided March 14, 2000).

"drawtite.com" for bonafide offers of goods and services to demonstrate a legitimate interest in the disputed domain name. The complainant failed to rebut this evidence, and lost the case.[18]

Conversely, in a case relating to bad faith registration and use, *Libro AG v. NA Global Link Ltd.*,[19] the respondent averred that it registered libro.com because it is the Spanish and Italian word for "book". The WIPO panel found that explanation acceptable prima facie and, therefore, did not find the registration to be in bad faith. Interestingly, the panel commented- "[the respondent] knew or should have known of Complainant's trademarks."

MASS REGISTRATION OF DOMAIN NAMES AND THE 'BROKER' ISSUE

Adding fuel to the fire of cyber-squatting, many brokers offer to register a whole set of domains for individuals, making it all the more difficult for arbitration panels to decide on the case. The most controversial cases on such registrations include the ".tv" registrations. The ". tv" country code exists for the small island of Tuvalu and has recently seen a spurt of activities from television companies seeking the domain for identifying their television channels.

THE SCENARIO IN INDIA

Indian Courts have been fairly active in deciding domain name disputes after seeing a spurt in litigation in recent times.

One recent case that has attracted much media attention is that of *Yahoo Inc., v. Akash Arora and Netlink Internet Services*,[20] a case pertaining to passing off in particular and abuse of domain names in general. Passing off generally involves disguising goods by a rival manufacturer to resemble well-known products or brands. In the Yahoo case, Akash Arora registered a domain titled 'yahooindia.com' and 16 domains with variations of the word 'yahoo' with Netlink

---

[18] Also see, *Digitronic Investionering v. @StocNet Registered*, WIPO Case D2000-0008 (decided March 1, 2000).

[19] WIPO Case D 2000-0186 (decided May 16, 2000).

[20] 1999 PTC (19) 201

Internet Services (NSI) in November 1997. Yahoo Inc., owns the globally known domain 'yahoo.com.' The plaintiff objected to the use of the word 'yahoo' in the domains registered by Akash Arora with NSI. The defendants in turn included a disclaimer on 'yahooindia' that the site had no connection with Yahoo, Inc. of California, U.S.A. The defendants thereafter activated their website and adopted substantial parts of the plaintiffs' Singapore website named "http://www.yahoo.co.sg/" which contained a section on India. The defendants argued that yahooindia.com offered India-specific content and that there was no protection for services in India and that no goods were involved in this case as is required by the Trademark Act. Furthermore, the defendants argued that 'yahoo' was a generic name and that no protection can be given for a generic name under the Trademark Act.

The Delhi High Court remarked that trademark law applies equally to domain names on the Internet, though the Indian Trade and Merchandise Marks Act does not contain any provisions that would apply to the case. The Court also held that where the parties are in the same or a similar line of business, the use of similar names would result in confusion and deception. The disclaimer entered by the defendants on yahooindia.com did not reduce the likelihood of confusion among Internet users. Also, in this case, the plaintiff Yahoo Inc. had obtained registrations on the trademark YAHOO and variations thereof in 69 countries, and that the mark was widely publicized and well known. The Court's most interesting reasoning was the fact that though "Yahoo" was a dictionary word there was no reason to deny protection for the mark. The court also held that though Internet users were technically educated and literate, this would not reduce the risk of confusion between the two sites.

In *Rediff Communications Ltd. v Cyberbooth,* the defendant adopted the domain name "Radiff.com" despite the existence of the well known website of the plaintiffs "Rediff.com". The court commented that such an adoption by the defendant completely dishonest and held that once the intention to deceive is established the court would not make any further enquiry whether there is any likelihood of confusion or not.

In contrast, the Delhi High Court had to decide on two competing domain names- "mutualfundindia.com" and "mutualfundsindia.com"

The Delhi High Court accepted the contention of the defendants that the word "mutual fund" was a generic name and ownership of the same cannot be vested in one person and no one can claim a monopoly over the said word.

In the 'bodacious-tatas.com'[21] case a WIPO decision under the UDRP, the panel ruled for the cancellation of the domain name. The action was brought by Tata Group India, holding a trademark on "tata". The panel ruled that the Tata trademark "deserve[s] wide protection due to its aura of high repute, and that bodacious-tatas, [...] was confusingly similar to the Tata trademark."

CONCLUSION

It is increasingly becoming difficult for cyber squatters and cyber pirates to hold domain names for 'ransom.' What we are witnessing is the global strengthening and unification of intellectual property regimes, tackling diverse disputes in a new medium called the Internet. Trademark owners will not have to show a commercial use by the domain-name pirate, at least not in the classic sense of providing actual goods or services. Instead, the intent to extract a ransom will likely suffice.

With respect to India, the Trade and Merchandise Marks Act lacks teeth since it applies only to goods (goods being defined under S. 2[g] of the Act to mean anything which is the subject of trade or manufacture). Recent amendments are being proposed to the Trademark Act that will see the introduction of service marks in India. At present, India relies on common law interpretation to solve Trademark cases pertaining to the Internet; especially ones relating to domain name disputes.

Recent legislative interest has resulted in amendments being proposed to the existing Trademark law. Major developments include:

1. Recognition and availability of service marks

---

[21] Available at http://arbiter.wipo.int/domains/decisions/html/d2000-0479.html. For the views on the case by Tata Sons see, http://www.tata.com/tata_sons/releases/20000828.htm. Another (interesting) site keeping track of domains that have been lost on account of applying the UDRP see, http://www.ousted.net/.

2. The Bill also proposes to increase the period of protection to ten years.

3. The Bill includes the concept of dilution of trademarks in respect of "well known trade marks". Any mark which takes unfair advantage of or is detrimental to the distinctive character or repute of a well known trade mark cannot be registered and such use would amount to infringement of a registered well known trade mark. Even advertisements against a registered, well known trademark that is contrary to honest practice in industrial or commercial matters, or is detrimental to the mark's distinctive character or works against the reputation of the mark will constitute infringement of the mark.

4. Trademark infringements are now cognizable and non-bailable offences. The bill now empowers a police officer to search and seize without warrant the goods, dies, block, machine, plate or other instruments or things involved in committing the offence.

The sooner individuals and businesses acquire legislative endorsement on the protection of domain names, the fewer will be the numbers involved in litigation, and the harder will it be for cyber squatters and pirates.

• • • • • •

- ***"What do you speak so loud I cannot hear what you say."***

Abraham Lincoln.

Information Technology and Legislative Design

Nandan Kamath:

Nobody would disagree with you if you were to say that one of the biggest events of recent times has been the surge in technology. Computers, the phenomenal growth of that network of networks called the Internet, mobile technologies like cellular phones and Personal Digital Assistants and who knows what next....

The use of these new modes of doing things for economic gain is an obvious fallout of the tremendous opportunities and advantages that these enabling technologies create and have to offer. More and more people got into it with some trepidation at first. As a result of increased transactions and the creation of new markets, there was a lot to be gained (by) all, and soon everyone wanted to jump onto the bandwagon. But with new technology also came new ways of interference by some elements, namely criminal hackers, who knew the technology too well and could find holes in anything and were ready to misuse this depth of knowledge for criminal purposes. Still, it did not make economic sense to let these unruly elements get in the way of the information revolution – there was just too much to be gained. This is where law found its role – it attempted to strike a balance and foster an environment in which people felt safe and could interact using technology with confidence. To achieve this, the legal framework supporting commercial transactions needed to be reinforced with consistent and predictable rules.

India's rather belated legislative intervention – the Information Technology Act of 2000, is now in force and even has Rules enacted under it.

The Act not only transforms the UNCITRAL Model Law on Electronic Commerce into domestic legislation but also brings in a detailed procedural infrastructure seeking to regulate this electronic marketplace.

A General Outline of the Act

The avowed purpose of the Act is to foster an environment in which laws are simple and transparent and in which the advantages of new technologies can be tapped.

It proposes:

Facilitation of

- Electronic commerce transactions,
- Electronic filing,
- Maintenance of electronic records and
- Electronic transactions involving the government

The Act provides for a legal framework so that the information is not denied legal effect, validity or enforceability solely on the ground that it is in electronic form. This is done by validating and authorizing the use of:

- Electronic data interchange (EDI),
- Electronic records and
- Electronic signatures

It adopts a 'functional equivalent' approach whereby paper-based requirements such as 'record', 'document', 'signature', etc., are replaceable with their electronic counterparts.

The Act also deals with issues subsidiary to this secure electronic environment such as privacy, contraventions relating to electronic transactions and information technology offences. It also seeks to set up various authorities to help regulate an information technology regime.

The Act not only lays down new substantive law but also makes incidental and consequential amendments to the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 to maintain its "functional equivalent" approach.

In summary, the Act deals with the following issues in some detail:[2]

- Secure electronic transactions – these enable parties to enter into electronic contracts
- Attribution of electronic messages, i.e., once the message leaves the information system of the originator of the message it is attributed to him.
- Electronic signatures and electronic records given legal status. In furtherance of this, and to maintain security of information, the Act establishes a Digital Signature Infrastructure making specific use of the Asymmetric Crypto System Technology with new authorities such as the Controller of Certifying Authorities being set up.
- 'Contraventions' regarding electronic records, viz., hacking, theft of electronic records, manipulation of records, spreading viruses, etc. have been defined. Involved in the inquiry and determination of the result of the proceeding is an adjudicating officer, appointed by the Government and possessing wide-ranging powers.
- Information Technology Offences, viz., tampering with computer source documents, obscenity – A limited number of offences have been created under the Act. These will be tried as any other criminal offences are under the Criminal Procedure Code but with unique provisions for investigation, search, etc., provided in the Act.
- Right of government bodies to decrypt information has been specifically given herein.
- Privacy and confidentiality of information submitted to statutory authorities – dissemination to third parties of such information collected in pursuance of powers under the Act is made a criminal offence.
- Facilitates e-commerce as well as electronic filing and maintenance of records as against the government.
- Setting up of new authorities/regulatory infrastructure - Cyber Regulatory Authorities such as the Controller of Certifying Authorities and the Cyber Regulations Appellate Tribunal (CRAT) have been established. The Act also seeks to set up a Cyber Regulations Advisory Committee (CRAC).

- Liability of Internet Service Providers (ISPs) for content on the Internet is limited in so far as the provider exercises all due diligence. This is relevant in connection with copyright violations, pornography, etc., residing on various webpages or moving through the systems of the ISP.

The "Functional-Equivalent" Approach

As mentioned earlier, the Act is based on the recognition that legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication. The "functional-equivalent approach" is based on an analysis of the purposes and functions of the traditional paper-based requirement with a view to determining how those purposes or functions could be fulfilled through electronic techniques.

The approach is to give legal recognition to the electronic counterparts of notions such as "writing", "signature" and "document", with a view to encompassing computer-based techniques that are able to carry out the same or similar functions. The Act does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria, which, once met by data messages, enable such data messages to enjoy the same level of legal recognition as their paper equivalents that perform the same function. The idea is that this must be carried out without necessitating the wholesale removal of the paper-based requirements themselves or disturbing the legal concepts and approaches underlying those requirements. As a result, the Act is supplementary to existing law rather than being a law to replace existing law.

How should the law approach technology?

Given above is a brief overview of this new legislation. What is instantly perceivable to anyone examining the legislative model in a little more depth is the significant emphasis on procedural details and the setting up of a regulatory infrastructure for digital signatures.

This leads one to the fundamental issue of this short article – what should be the interaction between developing technologies and the laws that seek to govern them?

Lead laws and lag laws

Very simplistically, all legislation can be pigeonholed into two categories – "lead laws" and "lag laws".

"Lead laws" are those that are preemptive – they are put in place to bring about changes, be they social, economic or technological. They are made on the assumption that law is a powerful tool for change and that circumstances and situations can be moulded through the establishment of the requisite legal models.

On the other hand, "lag laws" are reactionary in nature – they are enacted in the light of some particular problem or circumstance that has cropped up.

Although there may be only a very fine line of distinction between these two models the distinction has a functional utility when we look to examine how one would like the law to react to technology and how the law can facilitate technology.

It must be understood that much of technological progress happens through private initiatives in research and development and information is not easily available to legislators at intermediate stages of this development process. This makes the pitch queer for the law, as it cannot run side-by-side with progress. It needs to wait for the final product before being exposed even to the very fundamentals of the technology itself.

In this context, it would be safe to say that much of technology legislation takes the reactionary approach because until and unless the complex technology is understood and the possible ways in which this would challenge existing principles are fathomed, law often cannot react satisfactorily. As crucial, is the requirement that law should act with discretion, keeping open the possibilities of positive technological progress. This means that laws should not be too complex and detailed. On the other hand, neither should they be so flimsy as to lack

the certainty and predictability required of a law regulating and governing a specific technology.

In summary, technology laws are largely "lag laws". But many feel that, at the same time, they have a "lead" role too – by giving impetus to possible growth of positive trends in technology by being general enough to be facilitative in effect. While this "lead" objective might not envisage detailed procedural preemptive legislative strategy, it does imply the need for a non-intrusive, well-balanced legislative model that is specific enough for the moment and general enough for the future.

This brings us to the matter at hand – should legislative models be "technology neutral" or "technology specific"? Moreover, does the answer to this question vary with the type of technology and its practical application?

Technology neutral and technology specific law making

It is said that wisdom comes only from experience. There is no reason why this should be any different for the oft-cited "legislative wisdom". When lawmakers are faced with a fledgling field such as technology to deal with, they are no more experienced than anyone else. They slowly try and come to terms with the way to legislate in such a fast-changing world. But one of the foremost decisions they need to take is the type of approach they favour for legislative design and this involves certain policy choices.

The first real issue that encounters them is whether they should proactively promote a particular technology or simply leave it to grow on its own. Most legislators have felt the need to legislate citing existing legality requirements as being barriers to further growth and development. Further, they believe that the whole process could do with some impetus provided by the law, on the assumption that law can provide a degree of certainty and confidence for the various actors.

Secondly, having answered the primary question in the positive, they are faced with the question of how specific to get with the legislative response to particular technologies and techniques. This raises the debate between "technology neutral" and "technology

specific" approaches to law making. This is what the rest of this article will deal with.

The entire debate stems from the feeling that legislative approaches to new technologies must find the right balance between the goal of being flexible and time resistant and that of providing certainty through the prescription of specific details. This question arises in the context of the Information Technology Act, 2000 where legislation supports a particular technique of digital signatures (Public Key – Private Key signatures based on a Trusted Third Party Infrastructure) while ignoring, for the moment, other methods of providing electronic authentication. We will focus the debate between technology neutral and technology specific laws around this issue.

Technology Neutrality

Neutrality is the absence or lack of favour. Similarly, technology neutrality refers to the legislative policy or principle that guarantees non-discrimination practices in favor or against a given technology or technique. For example, when one is legislating on an area such as digital signatures using the "technology neutral" approach, one would refer to "signature devices", or the like, rather than specifically mentioning Public Key Infrastructure (PKI) based systems and legislating in detail based on the assumption that this is the only technique that will be used for authentication purposes.

Proponents of this view would have us believe that favouring, through legislation, one particular technology or technique will mean that innovators would be hesitant to develop more diverse, and possibly better, technology for fear of lack of legislative support. Also, it rests on the understanding that it is realistically impossible for anyone, including regulators, to forecast which technologies will succeed and which will fail and hence that it would be premature to legislate based solely on an existing technology/technique without looking at future/potential developments.

There is this belief that legislation and regulation, once enacted, have a tendency to be change resistant even when the need for amendment or deletion is indisputable. In addition, there is a risk that government may be setting one technological approach above other

existing or potential approaches and that may have the effect of distorting the natural market flow toward better products, services and more competitive pricing. With this understanding, the technology-neutral approach refers to legislation, which permits the use of methods in instances where otherwise a legal requirement of form could not be met, but does not specify any technique or implementation of a certain technique. This is a rather minimalist approach to law making where the law is seen only as a framework for technological growth. It does no more than act as a supporter/facilitator. What often tends to happen is that the law will be open ended, principle based and broad, and authority will be delegated to administrative bodies to issue more detailed rules on specific matters. It is felt that through this we can ensure flexibility and avoid premature endorsement of a particular technique (it is far easier to update administrative rules than it is to amend legislation).

When policy-makers support the notion of "technology neutrality," they undermine standardization of e-commerce infrastructure.

However, it would be far from the truth to say that all is hunky-dory with "technology neutrality". This legislative technique probably has as many critics as it does supporters.

Critics of the approach believe that it hardly serves the purpose; that it actually fosters legal uncertainty rather than the predictable and clear system that it professes to aim for. Moreover, they believe that the language of neutrality may actually undermine support for an already proven and available technology. They state that the law should not compromise the present while looking out too much for the future. While it may have a role of fostering a growing environment there is also the more immediate need to deal with an exiting phenomenon or technology. Technology neutrality fails miserably in this regard.

One of the strongest critiques comes from Michael Baum, vice president, Practices and External Affairs for Verisign, (one of the leading certification agencies throughout the world). He states, while commenting on calls to avoid Public Key Infrastructure (PKI) based legislation:

> "Technology neutrality is more a political buzzword than a clearly defined legal concept. In its most common usage, it refers to laws, regulation or other types of rules which purport to favor neither PKIs nor other technologies. The myth advanced by the technology-neutrality lobby is that such rules will ensure the unfettered development of diverse information security technologies and solutions, ensure mutual recognition of e-commerce transactions, and prevent non-tariff trade barriers to global competition for e-commerce services. But myth is not reality. Those who argue that e-commerce policy must exclude specific legal support for PKI in the name of technology 'neutrality' are in fact seeking to preserve a market for various other technologies --- technologies that have not yet been invented or demonstrated to be technically sound or practical for the needs of secure e-commerce. Thus the language of 'neutrality' is sometimes used to undermine support for an already proven and available technology."[3]

Technology Specific legislation

So what is the alternative? Clearly, the critics of technology neutrality call for more technology-specific legislation. For example, they would rather have us enact comprehensive digital signature legislation with specified requirements and loss allocation rules for a system where security, at least in part, is based upon a trustworthy PKI. While this may be cited as a case of over-regulation, these rules might be absolutely essential in order to foster trustworthy systems Further, it is argued, there is nothing that will prevent legislators from addressing non-PKI techniques as and when they crop up. This issue here is that PKI has been the tested and proven standard for digital encryption and certification. Why shouldn't there be legislation on this?

Baum urges[4] urge that the new economy brings with it new threats and this means we need more specific rather than more general law making. Most interestingly, he makes an interesting case for specific law making in the information age:

"An analogy can be drawn to the electric power and communications industries. Could we imagine failing to consider separately the specific technologies used to generate electricity, such as that generated from nuclear power plants versus that generated from geothermal turbines or windmills? Similarly, could we imagine neglecting to develop laws specifically governing communications satellites (or even the telephone) and relying instead solely on existing generic telecommunications legislation.....? The inherent complexity of information security, particularly within the context of the Internet, parallels that of electric power and other technologies where policy makers have seen fit to regulate some specific technologies (i.e., nuclear) for the public good, without stifling the development of other promising technologies and markets."

Next comes the issue of interoperability. Although, this does stem from the argument for certainty, it is a critical component of the new age economy. Technology thrives on wide and varied use. For maximum utilization, it is important that a particular technology is capable of interacting with others, being the basis for further growth, etc. This can happen much more easily if there is a uniform and general acceptance. What makes this easier is a sense of standardization. Laws validating and recognizing a particular technology or technique can only assist in this process of widespread acceptance by users and other developers in the industry. To achieve this sense of interoperability, it is crucial to specify implementation criteria and to do so at a level more detailed than abstract policy can possibly provide. Minimalist legislation just will not do.

In summary, those in favour of this technology specific legislative approach believe that the continuing expansion of new technologies requires a known and reliable system with established legal consequences. They believe that this would result in legal security through a detailed statutory alignment after having systematically considered the strengths and weaknesses of the particular technology or technique. Moreover, this amount of certainty would prevent the courts from having to develop case law on the subject.

An Intermediate approach

So far we have considered the two extreme approaches of technology neutrality and technology specific legislation. However, an interesting third approach is one that looks at the particular situation and then deems whether it is one fit for technology neutral or technology specific legislation.

Here we may refer to a 1998 Memorandum *Legislation for the Electronic Highway* that emerged from the Dutch Cabinet.[5] The Memorandum lists certain circumstances, in which it believes that technology specific provisions would be appropriate:

- In cases where these provisions define the extent of a regulation,
- In cases where legal subjects need insight in a (complicated) technology,
- If technology-neutral rules provide insufficient, little or no hold regarding the rights and duties of legal subjects, and
- In cases where these provisions are necessary to determine the conditions for government infringement of the legal subjects' rights and duties.

This is interesting because it is a functional approach to legislation, one that needs serious consideration.

The Information Technology Act, 2000 and Legislative Approach

The way the IT Act establishes the digital signature infrastructure and validates PKI leads one to believe that a technology specific approach has been adopted. Many quarters have criticised this as being too rigid.

The Act seems to have considered PKI as the only valid means of authenticating records and transmission having only given legality to this technique. What of biometrics and other developing techniques? Will the Act consider these only once they have been proved as reliable methods of authentication and are widely accepted? On the other hand, can one really expect these to receive wide acceptance without legality? Or will legislators just wait for technological

developments in other countries before making a decision on whether to validate newer techniques? These are all questions that come immediately to mind.

It is clear that in adopting PKI as the sole means of authentication of electronic documents and records, the lawmakers were keen to introduce an industry-standard. This is reasonable. But is the legislative model right?

In conclusion, it is submitted that the IT Act would have done well to have a more general approach in its text along the lines of the 1999 revision of the UNCITRAL Draft Uniform Rules on Electronic Signatures.[6] Details and specifics of the particular technology (PKI) could have been left to the Rules drafted under the Act. As they stand today, the IT Rules only elaborate procedures already specified in the parent Act.

The Act could very well have mentioned that all secure/reliable/enhanced electronic signatures are henceforth given legal effect/validity, leaving the determination of what constitutes a secure/reliable/enhanced to the wisdom of administrative authorities who could bring these into effect through the IT Rules. This would end up being more flexible and less cumbersome. For example, it there was a breakthrough in electronic signature technology (it would be a safe bet that someone somewhere in the world involved in late stages of development on such technology) that would have the potential to transplant PKI as the major technology, the law as it stands would require amendments that could only be done by the legislature. This could result in delays and in a 24x7 industry[7] in which literally every second counts; there could be significant economic losses that result. It makes eminent sense to use the device of delegated legislation to both retain the flexibility of technology neutral laws and also have the required specificity for legal actors to be sure of their rights and responsibilities in the existing scenario.

Is this a case of the legislature over-regulating or is it prudent lawmaking in this area of law where nothing can be classified as predictable enough? Only time, and experience, will tell.

Balliol College, Oxford University, UK. E-mail: nandankamath@hotmail.com

2 For a detailed analysis of the effect of the Information Technology Act on specific areas of the law *see*, Nandan Kamath (Ed.), *Law Relating to Computers, Internet and E-commerce: A Guide to Cyberlaws and the Information Technology Act, 2000*, Universal Law Publishing Co. Pvt Ltd, Delhi (unilaw@vsnl.com).

3 Michael S. Baum, Monograph entitled Technology Neutrality and Secure Electronic Commerce: Rule Making In The Age Of "Equivalence" – available at www.verisign.com

4 Id.

5 *Cited from*, Baum, *Supra*., n . 2.

6 A/CN.9.WG.IV/WP.84 available at www.unictral.org

7 A 24x7 industry is one that works 24 hours a day and 7 days a week.

.....

"Tomorrow is the most important thing in life. Comes into us at midnight very clean. It's perfect when it arrives and puts itself in our hands. It hopes we've learned something from yesterday."

- John Wayne.

The Information Technology Act from a Practical Perspective

_ankit majmudar

The Information Technology Act, 2000 ("IT Act") is supposed to have opened new vistas in the field of commerce. Ranging from securities trading on the Internet to the possibility of creating whole new means of storing information, the IT Act is supposed to make provision for it all. To an extent, no doubt, this is true. The IT Act does attempt to provide for a number of aspects relating to e-commerce and e-governance, and it a matter of justifiable pride that we are among the first few countries in the world to introduce a statute in this area.

Yet, as will be elaborated in the course of this article, the statue is not a cure for all the pitfalls that may and will face us in the course of adopting to the "new economy". In fact, there are a number of areas where the statue has not provided for any measures whatsoever, and still others where whatever it has done is, to say the least, impractical.

Principal Areas:

From a purely legal perspective, there are two segments where the contribution of the IT Act attains significance. The first, of course, is that of "digital signatures"; the second, and to an extent less glamorous, though certainly equally important, contribution of the IT Act is the changes it has wrought in the law of evidence. These are the areas to which this paper has devoted most of its attention.

Digital Signatures:

Signatures in general: functions and importance

It is fundamental assumption of the law of evidence (clearly reflected in section 22 of the Indian Evidence Act) that the written word is favoured by a court of law in preference to the spoken word as a piece of evidence. Thus the use of a signature serves as the principal evidence of a person's involvement. Traditionally, the functions of a signature on a document received by another party were manifold; they identified the sender, served as proof of the person's personal

involvement, associated contents of the signed document with the signer and attested to the intention of the party to be bound.

Today, however, a signature no longer finds place on every written communication that we send. E-mails don't carry signatures, and yet there certainly does exist a requirement for something that serves the same functions as signatures. Thus have evolved the new substitute to signatures- digital signatures.

At the moment, we are mostly concerned with the second characteristic, i.e., the absence of a handwritten signature. While even in today's e-days, most persons prefer to execute final documents on paper and obtain the written signatures of parties, one cannot ignore the role of electronic documents in the correspondence preceding and culminating in a written document. Thus, in a transaction of sale or purchase, or in the course of negotiating a contract, while the final document may be set out on paper, the correspondence that has been exchanged between the parties, which may have vital bearing on the interpretation of the contract itself, or in reflecting the intention of the parties, is often in an electronic format. There is a strong need, therefore, to develop a substitute for the handwritten signature, which can be used as sufficient evidence in any legal proceedings.

Digital signatures aim at filling this need, i.e, creating functional equivalents for the types of signature requirements used at present. Thus, the IT Act states the object of the Act to be , inter alia the recognition of transactions involving the "use of alternatives to paper-based methods of communication and storage of information"

Working of Digital signatures

As we have noted above, the basic function of a digital signature is to identify the author of the document and confirm that he approved its contents. This serves to protect the sender against false denial by the recipient that the data has been received; and to protect the recipient from false denial of the sender that the data has been sent out. Without such verification, a party may be able to unilaterally modify his or her obligations under a contract.

Digital signatures essentially work through encryption. Encryption as such, is of two types- symmetric and asymmetric.

Symmetric encryption occurs when the originator creates a message for a receiving party using a cryptographic process. The receiving party in turn uses the inverse process to obtain the true text. Any third party must have access to the inverse process itself to decrypt. However, the problem with symmetric encryption is the absence of a secure process to transport the knowledge of the inverse process itself to the receiving party.

In asymmetric encryption, on the other hand, a private "key", which is available only to the sender, is used to encrypt the document and a freely available public key is used to decrypt it. In theory, one can be derived from the other, since they are inverses. But in practice, it is computationally infeasible to derive the public key from knowledge of the private key within any reasonable period of time.

In this regard, one may refer to section 2(f) of the Information Technology Act, which denies an asymmetric crypto-system as "*a system of a secure key pair consisting of a private key for creating a digital signature and a public key to verify the digital signature*"

Again, "key pair", is defined to mean, "*in an asymmetric crypto system, means a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key;*"

Before digitally signing a document, a person must create a private-public key-pair. Since the public key must be known to a number of people, it has to be published or available in an on-line repository or a public directory.

The process itself (section 3 of the IT Act) works as follows: to sign a document, first delimit the precise areas that one wants to sign. This portion constitutes the "message". Then a hash function in the software computes a hash result that is unique to the message.

Hash function is an algorithm that creates a digital representation or compressed form of the message through a mathematical process. This is smaller than the message but still unique to the message. Hash functions themselves are public. The function takes the message as input and always gives the same string as the out

put, for the same message. The signer's software then transform the hash result into a digital signature using the private key. The resulting signature is therefore unique to both the message and the private key used to create it.

The reason for encoding only the hash result is that encrypting the whole message takes a lot of time. So only encrypt a finger print of it, so that when the excerpt that is finger printed is much smaller than the original text.

Verification, in turn, is done by computing the hash result of the message using the same hash function. Then the newly computed hash result is compared to the original hash result obtained from the decryption of the digital signature through there public key. Verification is therefore done by comparing the "fingerprint" obtained by decoding the signature with the "fingerprint" obtained from the text of the message. Any change to the message will alter the hash function, thus ensuring that the original encrypted hash function does not match with the hash function obtained from the message by the receiver. Forgery is therefore prevented; a forger cant encode because he has the hash result but no signature key; nor can he attach a signature because the hash function is different .

Thus, a verified message shows that (1) the message was sent by the owner of that private key (otherwise decryption was not possible) and (2) that the message was unaltered.(see section 2(zh) of the Act.)

However, as is apparent form the above, digital signatures therefore, are not connected to confidentiality. The signature is attached to the text and the message is left untouched.

The Act defines a secure digital signature as a digital signature to which, by the application of a "security procedure" agreed to between the parties concerned, it can be verified that the signature was unique to the person affixing it and capable of so identifying him, etc - i.e., was a valid digital signature. But "security procedure" is defined to be one prescribed by the Central Government. So how can parties agree to it? There would appear to be some measure of ambiguity in this regard.

Certifying Authorities: these play a role in associating a person or entity to a particular key pair. The Act defines them as "*a person who has been granted a license to issue a Digital Signature Certificate under section 24*".

Certifying Authorities would be appointed by the Controller, who is a Governmental Authority appointed under the Act. The Principal function of a certificate so issued by a Certifying Authority is to bind a public key with a person. It would list the two, so that a person can use the key to verify the signature. The Certifying Authority's certificate would be signed by its own digital signature – which can, in turn be verified with a public key issued by an other authority (under the IT Act, the controller). These certificates would be available in an on-line repository. A public repository can also contain information such as notice of loss of or compromise of a digital signature. For this purpose, it would be appropriate for digital signatures to be time stamped; i.e., have an attestation that a document was in existence at a particular time, so as to allow for the suspension of a digital signature from a particular date.

Evidential aspects of the IT Act:

Prior to the IT Act itself, section 610A of the Companies Act specifically allowed for the admission of documents stored on computer media, subject to certain conditions concerning the reliability, etc, of the information. Besides this, however, there were no provisions specifically allowing the admission of computer generated documents in a court.

Today, tremendous use is being made of the internet in business relations. And any dispute involving the internet will require the admission of evidence stored on a computer. The Evidence Act earlier allowed for use of secondary evidence to prove documents and includes within the definition of secondary evidence, "*copies made by mechanical processes*". But there was nothing specific as to evidence generated by computers.

While there was nothing allowing for the admission of such evidence, there was nothing preventing it either - therefore, there were no formal requirements as to the qualifications of the systems required

for generating such documents, the working of the computer, etc. Further, it was not clear if information stored on a computer was a "document". The definition of "document" under the Evidence Act spoke of matter "expressed or described upon any substance..." - a definition that could be interpreted to include or exclude electronic documents. Another issue was that of copies vs. the original. In an electronic document, what is the original and what is the copy? But under the law of Evidence, copies of documents are not always admissible. So how does one determine what constitutes the original.

Amendments made by the IT Act in this regard.

The amendments made by the IT Act affect four legislations: the IPC, The Evidence Act, the Banker's Books Evidence Act and the RBI Act. In the context of evidence specifically, however, the relevant amendments were those to the Evidence Act and the Banker's Books Evidence Act.

Evidence Act

The principal amendments to this are broadly as follows:

"Evidence"- the definition has been broadened to include "electronic records". Typically, oral admissions as to the contents of documents are not considered relevant evidence by the Court. Now, the same bar is made applicable to electronic records as well. Again, documents are broadened to include "electronic records" specifically.

Provisions exist allowing the court to consider evidence of persons familiar with the handwriting of the person when the court attempts to form an opinion as to the person by whom a document has been written or signed. So an analogous provision has been inserted, which would allow the Court to consider the opinion of the certifying authority when the court considers the digital signature of any person.

The manner of proving electronic records has also been provided for. This allows for the admissibility of the contents of an electronic record and gives them the status of documents and makes them admissible, subject to certain conditions[1].

[1] These conditions basically require the computer to have been regularly used for storing the information that is sought to be proved; that throughout this period the computer was working properly, the information is derived from information fed into the computer in the ordinary course. Further, if a number of computers were used for

Section 67A provides for proving that the digital signature on the document is the signature of the subscriber, except when it is a secure digital signature, i.e., when the parties have agreed to a security procedure to verify the digital signature (as per the definition in the IT Act). Otherwise, proof is by applying the public key obtained from the certificate produced by the certifying authority.

The IT Act also adds certain presumptions to the Evidence Act. While these are rebuttable, in the absence of any proof to the contrary, these would prevail. An example of these presumptions is

"Secure electronic records and secure digital signatures are presumed to be unaltered from the time that they were made secure and affixed by the subscriber with the intention of approving the record respectively."

Or in the case of electronic records that are more than five years old, it is presumed that the digital signature that purports to be the signature of a person was affixed by that person. However, given that some measure of the presumptions rely on "secure digital signatures", the definition of which itself rather unclear (see above), the amendments to the Evidence Act do not seem to fulfill all the expectations.

Amendments to the Banker's Books Evidence Act:

The Act itself earlier stated that the term "Certified Copy" included a copy obtained by mechanical or other process which ensured its accuracy. Therefore, this provision could have been used to bring in computer printouts.

Now the definition of "Banker's Books" has been defined to include not only ledgers, day books, etc kept in the written form, but also printouts of information stored on computers, and other such devices.

---

such processing, they be treated as constituting a singe computer. Additionally, the Act allows for the court to accept a certificate from the person occupying a responsible position in relation to the computers where he can certify the existence of these conditions

"Certified Copy" has now been defined to include certified printouts or copies of printouts of information stored on the computer, etc.

Such information is subject to the condition that the following certificates are provided:

(1) certificate from the principal accountant or branch manager;
(2) certificate from computer systems in-charge, certifying certain details and particulars as to the safety of the system;
(3) certificate from the computer systems in-charge that to the best of his knowledge, the system was working well at the appropriate time, etc.

Thus, the amendments specifically allow for the inclusion of computer based records and evidence, subject to the restriction that such information be certified as being properly maintained.

Rules:

Certain Rules have also been issued under the IT Act. The Rules clearly (at least, far more clearly than the Act), explain the process of digital signature creation and verification, highlighting asymmetric crytography, and the process of verification. Again, Rule 6 lists out the standards to be followed for the information technology architecture for certifying authorities. Rule 7 lays down the contents of the certificate, including the validity period, public key information, etc.

Rule 12 speaks of cross certification between Certifying Authorities, i.e., the digital signature certificate of one Certifying Authority is to be digitally signed by the signature of the certifying authority, which, in turn, is verified by the certificate of another certifying authority. It may be noted that the IT Act, in contrast, speaks of certification of the digital signatures of certifying authorities to be the duty of the Controller. There would appear to be some ambiguity in this regard.

Another piece of ambiguity arises in the fact that according to Rule 19(2), the guidelines specified in Schedule II to the Rules are "*... guidelines for certifying authorities.*"

These guidelines themselves, however, refer to "organizations" which have been defined in the glossary attached to the Rules to mean: "an entity with which a user is affiliated and could include a user". Further, Schedule III specifically says "security guidelines for certifying authorities". It is therefore not clear if Schedule II applies only to the Certifying Authorities, or to all organizations, including organizations who are merely using digital signatures. Since the guidelines are extremely stringent, it may be impractical to enforce them for all organizations, including those which are mere users under the IT Act. However, a clarification in this regard would be required.

Conclusion:

As detailed above, the IT Act has broken new ground in several areas . Yet, in many respects ambiguities continue. Until these are resolved, it is unlikely that corporates will be comfortable venturing into the world of e-commerce. Yet it would be worthwhile to remember that the Act has an important role to play in ensuring that only a particular type of evidence is admissible. Digital Signatures in general may not have the value they would be generally presumed to have unless they confirm to the specifications set out in the Evidence Act and the principles of the IT Act itself: thus, the standards specified in the Rules may have to be complied with, etc...failing which a digital signature may no longer have the validity it is supposed to gain under the Evidence Act, leaving the Courts to return to the realm of conjecture and uncertainty. Again, some of the requirements under the Act are difficult to comply with. For example, in case proving an offence of hacking, the hacker may have used multiple systems: would this mean that certificates have to be obtained with reference to all of them? Further, what if a malfunction in the system did occur, what if it did not affect the information itself? Would the information then be admissible?

These are the sort of issues that we will have to face even with the IT Act in force. Accusations that the Act is not a complete code on the area of information technology law, therefore are certainly not without merit. The Act does not even attempt to address certain issues, such as domain name disputes, taxation of e-commerce, etc. All these are still left open, possibly for future governments to regulate...and till then, it remains for the Courts to decide.

Hackers and Crackers And Our Legal System

Aditya N. Mittal
H.J.S.
Addl. Director (Research)

Expansion of Internet facility, while on the one hand, has enabled the user to get any information any time and any where, while on the other hand some "wild" elements have created problems to these web. sites. Web traffic is growing faster than almost any other type of data traffic over the corporate network as more and more users take advantage of this huge information resource, and more and more applications become web-enabled in some way.

Computer security law is a new field, not yet established in the realms of law. The meaning of most technical computer terms are still a bit foreign or unclear in the court rooms. The legal establishment has yet to reach broad agreement on many key issues. Even the meaning of such basic terms as "data" can be the subject of contention. Computer security law is still moving very slowly, and if it moves, it is mostly due to litigation coming to court and making lawyers and judges very much reluctant due to their lack of knowledge and understanding of technical terms and security issues.

The Indian Parliament has taken a lead by enacting Information Technology Act, 2000 under which cyber crimes, even committed out side India by any person, regarding Indian sites can be prosecuted in India. But only Parliament can not help unless our whole system of Administration of justice which includes Bench and Bar comes forward to prevent the cyber crimes. In America, the Science and Technology section of American Bar Association has formed speciality committees in several areas under the Electronic Commerce and Information Technology Division. Such speciality committees are:

A-The Cyber Notary Committee-

The Committee tries to address and recommend solutions to the discrepancies between international law and US law, which many

times turns out to be inadequate to practice due to the legal systems' differences, costs and liabilities. The advent of Electronic Commerce demands a more reliable authentication and certification system of electronic "documents" to assure the reliability and enforceability of underlying acts specially overseas. The Cyber Notary Office is a concrete initiative that aims to bring together the information technology and the legal expertise.

B-The Information Security Committee-

The Committee explores the computer security issues, included but not limited to those related to cryptography, risk analysis, standards and commercial reasonableness, and the relationship between security and the legal efficacy of electronic commerce.

C-Electronic Commerce Payment Committee-

This committee is dedicated to explore, consider the requirements of, and recommend on the legal solutions to meet the needs arising from undertaking electronic payments within the context of electronic commerce.

D-Judicial Electronic Data Interchange (EDI) Committee-

This committee considers the use of Electronic Data Interchange as a vehicle for administration of justice among information systems of two or more parties.

In the computer world Hacking and cracking is the greatest threat to computerized information after viruses. Intrusion is an attempt to break into or misuse of system. When an intrusion is from outside, it is a hack and hacking is done through internet. When one gets into some one else's computer system without permission in order to find out information or do something illegal is covered under the term "hacking". Tracing hackers and crackers is a very labour-intensive, specially with the former. The hackers are of various types:

Network hackers

Network hackers break the security of computer network, by using their skill in a way which is illegal. Their activities involve denial of service or entering a secure area by subverting its security cordon. Denial of service is attempted by flooding the web server with false requests for pages to engage it in processing such requests

leaving it no time to respond to legitimate requests and thereby affecting its ability to respond and perform its internal functions. Entry in the secured area in obtained by setting up programmes that tries million of passwords until one is accepted. They invade the private data and further invade the network to reach the sensitive data. once hackers get into the machines that host networks, they can alter and remove files, change information and erase evidence of those activities.

To elaborate more the hacker may be described as:

(1) A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.

(2) One who programmes enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.

(3) A person capable of appreciating hack value.

(4) A person who is good at programming quickly.

(5) An expert at a particular programme, or one who frequently does work using it or on it, as a Unix hacker.

In brief, they may however, be described best as malicious meddlers who try to discover sensitive information by pocking around.

Crackers

Cracking is another form of hacking. It involves breaking the security on software applications. Crackers develop their own software that can circumnavigate or falsify the security measures that keep the application from being replicated on a PC. For example, if a registry access is permitted to every one, passwords could be cracked. An employee could be able to dump password registry contents, if he is allowed access, and crack them at leisure. Password dumping and cracking are not difficult. Plethora of tools for that purpose are available on the Internet. Password having been cracked, it permits the cracker to log on to the server with the cracked user name and password. He then gains a legitimate access to the restricted system resources.

Thus, protection is needed against theft of equipment, loss of software or data, virus incidents, internal system attacks and hacking.

Loss software and data and virus incidents have been the main cause for loss of computerised information.

- Cyberpunks - They are the masters of cryptography.
- Phreakers - They combine their in-depth knowledge of the Internet and the mass telecommunications systems.

Virus incidents

Virus incidents have resulted in significant and data loss at some stage or the other. The loss could be on account of:

- Viruses;
- Worms;
- Trojan horses;
- Logic bombs

Viruses

A virus is a programme that mayor may not attach itself to a file and replicate itself. It can attack any area : from corrupting the data of the file that it invades, using the computer's processing resources in attempt to crash the machine and more. If that seems vague, it is because it is tricky. Virus incidents have been the main cause for the loss of the computerised information. There is a general awareness about these viruses and their harmful impact. All organisations protect themselves against these viruses through virus scanning software.

Worms

Worms may also invade a computer and steel its resources to replicate themselves. They use the network to spread themselves. "Love bug" is a recent example. It spread by making copies of itself and sending them out to listing in a victim's e-mail address book. It shut down many company and government net works.

Trojan horse

Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb.

Logic bomb

A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples.

The Law Commission of U.K. in its report suggested for reforming the present Law of Hacking as follows:

The possible criminalisation of conduct which is not at present directly covered by the criminal law must involve a consideration of whether it is in the public interest that such conduct should be regarded as criminal. This in turn may involve consideration of whether it can be adequately controlled in some other way, in particular by the civil law.

SHOULD THE OBTAINING OF UNAUTHORISED ACCESS TO A COMPUTER BY HACKING BE A CRIMINAL OFFENCE?

.....there are some special features concerning computers and their accessibility to which we think attention must be drawn at this stage.

(i) Computers are capable of storing and processing vast amounts of information. Information which twenty or thirty years ago might have been stored in large rooms full of filing cabinets can now be kept on a single disk smaller than a pocket sized note-book. The computer is a relatively recent invention which we must now accept as a feature of late 20th century life. In general, the benefits which this new technology has brought to members of society are not in doubt.

(ii) Much of the information stored in computers is information of a nature which those who disclose it to the computer owner would not want disclosed to third parties. For example, information relating to individuals of a personal kind, bank accounts, credit ratings, medical records and trade secrets.

(iii) For large computer systems to be effective, and to be of maximum use to legitimate users, including those who supply information to computer owners, they must be readily accessible from 'remote' computer terminals. This

necessarily gives rise to problems of security which are of an entirely different kind from those which arise in connection with the safeguarding of manual records.....it is difficult if not impossible to create a totally secure computer system.

(iv) It may be possible for a person to obtain unauthorised access to information stored in the computer without the need for any physical presence other than at a terminal which it connected to the computer system by means of a telecommunication system. Without this physical presence, a person who seeks to obtain unauthorized access will not be exposed to the risk of prosecution for offences such as burglary or criminal damage which might be applicable if physical access were required.

(v) In deciding whether obtaining unauthorised access to information held on a computer should be a crime, analogies with other forms of conduct may be helpful but can be misleading. It is probably better, therefore, to consider the computer for what it is.....

The arguments for an offence

One argument in favour of an offence.....acknowledges the importance of computers for society as a whole and suggests that those who use and rely on computers maybe inhibited from making full use of them, if they fear that others might obtain unauthorized access to information held on them. For this reason it is in the public interest that society must try to deter hacking generally, or at the very least in respect of computers holding certain kinds of information .

.....Further argument in favour of an unauthorized access offence....rests on the possible consequences of hacking to a computer system. Where the computer system is especially important, or the information stores on it especially valuable, these consequences will be more serious, but hacking could lead to an inadvertent damaging of any computer system. An offence of obtaining unauthorized access to a computer would signal society's disapproval of those who deliberately set out to breach security measures, and amount to a rejection of the claim that hacking is a harmless intellectual pastime. This rejection would have beneficial consequences beyond the number of successful prosecutions likely to be brought.....

Another positive side-effect of a hacking offence would be that its prohibition may serve to deter conduct which is made possible by amending the existing law.

For addiction to be a sufficient defence to a criminal charge, the individual should be affected to such an extent that the affliction may be viewed as a 'disease of the mind' sufficient to prevent the formation of the requisite *mens rea*, this would then effectively equate with a defence of insanity. Whether or not there is clinical evidence to support any finding of addiction to computer hacking is not a subject which can be debated here, although supporting evidence had been produced during the trial. It is certainly the case that at the trial Bedworth gave repeated assertions, not only that he had committed the acts at issue, but also that he was aware that these acts were wrong and would not be repeated. If he were truly addicted would he be able to make this latter promise ? Charlesworth,[1] citing the case of *Lawrence* [2] points out that courts are unlikely even to take addiction to account in mitigation. *Lawrence* was, of course, a case in which the offence (of burglary) was committed to feed the addiction rather than being directly related to that addiction. Whilst it can be problematic to draw analogies between such cases and those, such as *Bedworth*, in which the addiction is to the criminal behaviour itself, nonetheless there is confirmation for the absence of a general defence of addiction is *Kopsch* [3] - '[t]he defence of uncontrollable impulse is unknown in English Law'.

Finally, it is entirely possible that what acquitted Bedworth was 'the sympathy vote'. There was evidence at the trial that the police had utilized tactics such as 'drawn raids' on his home in their apprehension of Bedworth and it may be that the jury thought that he was only a young fresh-faced boy and that, in the particular circumstance of the case, the police had over-reacted.

---

[1] Andrew Charlsworth, Between flesh and sand : Rethinking the Computer Misuse Act, 1990 International Yearbook of Law, Computers and Technology, 1995, Vol.9, p.31.

[2] (1989) Crim. L. Rev. 309.

[3] (1925) 19 Cr. App. Rep. 50.

Whilst we can never be sure of the precise reasoning on which this acquttal was based, it is clear that no such sympathy was extended to his co-defendants, Strickland and Woods who, having pleaded guilty, were sentenced to six months' imprisonment – a recognition, perhaps, of the fact that the behaviour in question resulted in significant financial loss, can cause serious damage to the systems affected and should be viewed seriously.

Similarly, in the more recent case of *Pile* (above) the judge clearly took the matter very seriously and in the face of the likely losses to affected users, allowed a defence application to seek an expert opinion on the amount of damage caused by Pile's activities, in advance of deciding on sentence. This led to a sentence of 18 month's imprisonment when the case returned to Exeter Crown Court in November 1995. Neither has there has been much leniency for the latest case involving a schoolboy hacker, *R v Pryce*.[4] Pryce was fined a total of £1,200 for 12 counts of hacking into computer systems including that of the Pentagon whose network was said to be much easier to penetrate than that of UK University!

Even taking into account the provisions provided in the Computer Misuse Act.[5] a further problem which could have surfaced in the case of both Bedworth and Pryce is that of jurisdictional problems; some of the computer systems into which they hacked were in the other countries. The reverse situation is obviously equally likely : hackers in other countries can hack into computers and networks in the UK. How is this problem to be addressed? What of the virus which originates in the former USSR or Eastern Europe? The evidence is that this is being dealt with by co-operation between police forces, at least in Europe, and European Police forces have agreed with Interpol that hackers or originators or viruses can be prosecuted in their country of residence, even if the hack or the virus has wreaked havoc in another jurisdiction. This improved co-operation has now

---

[4] (1997) March, Bow St. Magistrates Court, See *Guardian* (1977) 22 March.

[5] Section 4 of the Computer Misuse Act 1990 makes it immaterial (subject to certain conditions detailed in subsequent sections and subsections (a) whether any act or proof of which is required for conviction of the offence in the home country concerned; or (b) whether the accused was in the home country at the time of such an act or event. See also *Demis Kelleher International Computer Crime (1997) 147 NLJ 445.*

been extended into Eastern Europe and has been finding ways of dealing with organized gangs – particularly in Russia and the Balkans. Indeed the evidence that many viruses originate in Eastern European countries with little regulation of such activities has been used as evidence of the efficacy of computer crime legislation – 'the thesis that lack of computer crime legislation tends to mean different ethical standards amongst citizens is, apparently, borne out by what is reported from Bulgaria. Bulgaria had the highest rate of computer virus production per capita of any country in the world. In Bulgaria, there is no computer crime legislation and there are no copyright laws.'[6]

In Malaysia, the Computer Crimes Act, 1997 (Act No. 563) defines the offence of hacking as:

Section 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.

(3) A person guilty of an offence under the section shall on conviction be liable to a fine not exceeding fifty thousand ringgit or to imprisonment for a term not exceeding five years or to both.

---

[6] Klaus Brunnstein and Simone Fischer-Huebner, *How far can the criminal law help to control IT misuse ?* International Year Book of Law, Computers and Technology, 1995 Vol. 9, p 111.

In India Section 66 (1) of Information Technology Act, 2000 defines hacking as:

"Who ever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means commits hacking."

There are two vital ingredients for mens rea to be applied to a hacker:

(1) the access intended to be secured must have been unauthorized, and
(2) the hacker should have been aware of the same at the time he tried to secure the access .

Hackers are becoming a menace so uncontrollable that even the largest companies in the world are finding it difficult to cope with their incessant attacks. Some hackers "enjoy" cracking systems and gaining access to them, they do not intend to commit any further crime. It is a question of debate whether such act in itself constitutes an offence or not.

Strategy for Prevention of Computer Crime

In light of proliferation of computer technology, the impact of computer crime have become enormous. Hence a multi pronged strategy is required to fight the menace to its logical end. The two main dimensions of the strategy are, systemic methodology and legal deterrents.

(a) Systemic Methodology

Computer crime is a new form of criminal offence that pervades through trans-national borders. Concerted international Co-operation is required to effectively address this crime.

International collaborations and exchange of technology pertaining to data security should be vigorously encouraged.

It has become imperative to develop concepts/ guidelines (manual) for computer security. The implementation of

such manual, at all levels within an organisation and between organisation, should be made mandatory. Such guidelines/manual when earnestly implemented, hold greater prospects of success than, enacting new legislations for data protection. It should be made obligatory on the part of companies/institutions to provide in their annual reports, a confirmation to the effect that data security standards as prescribed by the manual have been adopted.

A transaction oriented system need permit only 'read only' or 'inquiry only' access. This offers a greater degree of protection than a system offering access for programming.

(b) Legal Deterrents

Demarcation of the activities which constitute offences which are non-offences.

Amendment of the domestic criminal law (of all countries), based on an international understanding, to meet the requirement of prevention of computer related crime.

Effective prosecution, *inter-alia*, by adopting the existing criminal procedure law and related provisions.

The formulation and adoption of a procedure for the investigation of computer crime is cardinal to the effective translation into action, of any new piece of legislation or amendment/supplementation of existing law. The guidelines/rules should spell out the procedural aspects relating to search of the premises, seizure of incriminating documents/materials, the duty of witnesses etc.

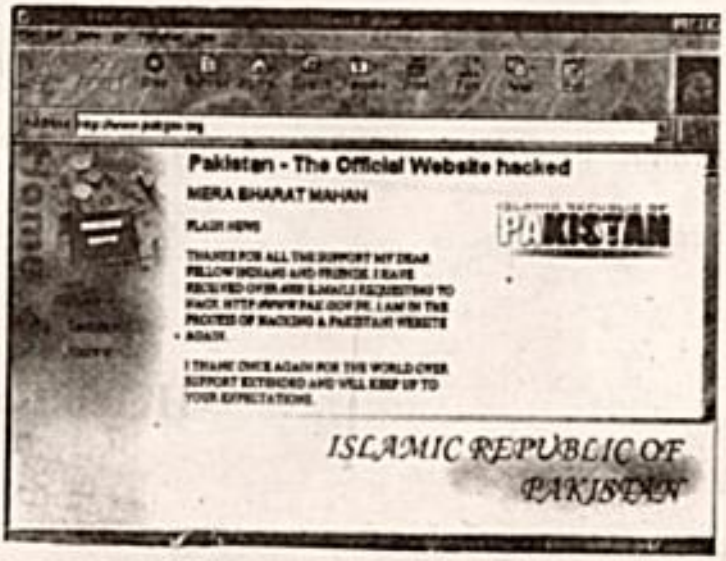
In addition to the above, considering the fast changing nature of computer-related crime, it is desirable to adapt the guidelines and classification suggested by the Organisation for Economic Co-operation and Development (OECD) with necessary amendments to suite national requirements.

In India, National Association of Software and Service Companies has set up the country's first anti-hacker organization named as "National Cyber Cop Committee". This Committee includes

Nasscom representatives, senior policemen and government officials apart from experts. The Cyber Cop Committee has tasked itself with monitoring cyber crime within and outside the country and coming up with recommendations to enable companies to protect themselves better against hack attacks. A hacker's greatest asset is that he can easily transcend all physical barriers and concept of countries has no meaning for a cyber criminal. Hackers are also helped by the fact that most countries are yet to come up with laws to counter cyber crimes.

Another important factor of hackers is that they are often quite young and possibly still at school and they attempt to gain access to other people's computers simply because of the intellectual and technical challenge which that activity presents. In the beginning, they access such other computers just for fun but soon they start breaking into computer systems at banks and siphoning-off money, while others stole credit card details and fraudulently use this information to make a quick buck.

Recently, on 22 December, 2000, an Indian hacker, who received about 6000 e-mail messages to hack official web. site of Pakistan, has hacked by using DNS hacking process, the official site of Pakistan as counter attack. The web.site appears as:



The Indian hacker has warned Pakistani hackers that he will destroy the whole internet system of Pakistan and Pakistan should never think of re-attack. The Indian hacker has given an option that who so ever wants to chat with him, may do so on 24th December, 2000 at 12.00AM at Yahoo Channel and he shall remain present there by the name "True_Indian_hacker". The hacker has also mentioned "Vande Mataram" and "Jai Hind" on each page.

Such incidents may be fatal for the defence as well as economy of any country.

The challenge has to be accepted by cyber professionals. Though various security systems like cryptography to firewalls have been invented but the holes still continue. Unless hackers are detected, the law can not take its recourse.

• • • • •

- ***"The best and most beautiful things in the world cannot be seen, nor touched....but are felt in the heart."***

-Helen Keller

LAW AND CYBERSPACE : WHAT IT PORTENDS FOR THE COMMAN MAN

T. K. Viswanathan[1]

If you don't own a computer or have not gone near one even by accident and if you believe that computers and Cyberspace are not for you, then read on, because this article is for you.

The Fantasy

> ***HAL: This mission is too important for me to allow you to jeopardize it Dave.***
> ***Dave: I don't know what you're talking about, HAL***
> ***HAL: I know that you and Frank were planning to disconnect me, and I'm afraid that's something I cannot allow to happen.***
> ***Dave: Where the hell did you get that idea, HAL?***
> ***HAL: Dave, although you took very thorough precautions in the pod against my hearing you, I could see your lips move.***
> ***Dave: HAL, I won't argue with you anymore. Open the doors.***
> ***HAL: Dave, this conversation can serve no purpose anymore.***
>
> ***Goodbye, Good afternoon gentlemen, I am a HAL 9000 computer. I became operational at the HAL plant inUrbana, Illinois on the 12th of January, 1992. My instructor was Mr. Langley, and he taught me to sing a song. If you'd like to hear it, I could sing it for you…. "***

2. The transcript of the above conversation between David Bowman and HAL, the legendary computer, is one of the most important scenes in the movie ***2001: A Space Odyssey*** which was released way back in the late sixties. Those of us who saw the movie were held spellbound by

---

[1] Member Secretary, Law Commission of India.

the special effects of the movie and a talking computer. It was a fantasy thirty years ago when PCs were for away in the future much less a talking computer!

3. But then human ingenuity has proved that nothing is impossible. Three decades later we have speech recognition softwares and computer synthesized voice which enables us to re-enact the HAL 9000 –David Bowman encounter in every home computer! Inventions and discoveries, accidental some of them might have been would not have been possible but for imagination and vision on the part of mankind.

The Fiction

4. The word Cyberspace was coined by Willian Gibson in his novel Neuromancer. Set against the backdrop of an imaginary 21st Century Japanese city called Chiba, the central plot of the story revolves around a computer hacker by name case. Case is a computer addict who makes his living by breaking into security systems. He is physically incapacitated by infliction of damage to his nervous system by means of a Russian wartime mycotoxin for stealing from his employer. His longing to regain his health and obsession for hacking leads him to strike a deal with another character in the novel called Armitage. As part of the deal Armitage pays off Case's debts, repairs his neural damage, and places him under the protection of another character by the name Molly, who turns out to be a professional killer. Case carries out a series of assignments with Molly and others at the behast of Armitage. Soon the truth dawns upon Case that he is a tool in the hands larger forces which were controlling his activities and it is Neuromancer, a far-reaching artificial intelligence which has been controlling him. Neuromancer drives home an important message that technology is powerful and it can control society without producing positive benefits.

5. By a strange coincidence Neuromancer was published in the year 1984 which was the setting or Orwellian classic 1984. The novel centers around Winston Smith a minor party functionary in one of the three warring states. He

lives in a society where the Big Brother is always watching its citizens and their thought read by the Thought Police. His longing for truth makes him a rebel and as a consequence he is arrested by the Thought Police and sentenced to imprisonment. He is tortured and re-educated with the result he loses his independent power of mental existence. Published in 1949 Orwell's 1984 made a deep impact upon the readers because it highlighted the dangers of totalitarianism. The dangers portrayed by Orwell may be exaggerated but with the evolution of technology like Clipper chip, Capston and Carnivore if sufficient safeguards are not devised, privacy of individuals are like to be invaded by the state agencies. More of it later.

The Virtual Reality

6. The fantasy and the fiction are set to become reality with the advent of internet. Started as a U.S. defence project in 1973 as research program to device interconnecting networks of various kinds to survive a nuclear attack which will destroy the momolithic central communication command in the early part of any war it was made available in 1983 to select users. Three technologies made internet possible. First was packet switching. Information is transmitted through the Internet using a technique known broadly as 'packet switching. Second was the development of a set of protocols knows as TCP/IP which enabled computers to exchange information regardless of their make origin or operating system etc. Third was the development of client-server technology which allows a computer to access and utilize service and programmes residing in another computer. The Internet Protocol address consists of 4 sets of numbers between 1 to 255 separated by periods. These are unique numbers which identify each computer in the internet. Since it is difficult for human memory to remember large digit numbers Domain Names were resorted to mask the numbers making it human friendly to remember and key into the computer to log on.'

7. Internet then is like bye lanes leading to lanes which in turn lead to streets then to roads and then ultimately into

highways sprawling across the globe. Internet is connected through a series of computers each with a different role to play at every level. Had technology stopped with this perhaps internet would have at best been another improved means of communication over teletext or fax. But the invention of hypertext markup language by Tim Berners-Lee working at CERN Geneva popularly known as HTML dramatically altered the whole scenario. His hypertext link is an electronic embedded address that points to another internet location in the internet. To jump to that location all a user has to do is to click on the hyperlink and automatically he is taken to that site by the browser. Basically a Mark up language is a computer language which describes how a page should be formatted. A web page also contains HTHL Tags that describes how the text should be formatted when the browser displays it on the screen.

8. Initially web consisted only of text but soon graphics took over with browsers like Mosaic. Netscape Navigator and Internet Explorer adding sound, graphics and other multimedia content to the web pages. With that it can be said that the Cyberspace has blossomed into medium of its own. The implications of this were not difficult to grasp. The prospect of sending messages and files across the continents with lightening speed and that to at a negligible cost was very appealing to most of us. It was only a question of time that entertainment industry and commerce should migrate to Cyberspace and that happened sooner than expected resulting in Convergence of technologies leading to blurring of the distinctions between broadcasting, internet and mobile computing.

THE LEGAL PROBLEMS POSED BY CYBERSPACE

Vanishing Borders and Sovereignty of Nation States

9. Nations have been exercising authority and jurisdiction over individuals on the basis or territorial nexus. This is the established principle of international law. Since Cyberspace is a borderless environment both the authority and the exercise of jurisdiction of the states over

individuals not within their territory are open to challenge. Karl Marx predicted the withering away of law and state for different reasons but it appears that Cyberspace will spell the doom of modern nation state. Considering the fact that modern nation state itself is a product or renaissance and reformation which broke the authority of the Church new forms of associations like virtual communities will emerge as alternatives to modern state. The most important and difficult problem which has to be addressed while dealing with regulation of Cyberspace is the question of identification of users in internet. Internet permits a person to acquire as many userids as possible without revealing his flesh and blood identity. This is further compounded by the fact that the problem of anonymity and pseudonimity which is rampant in Cyberspace. Assumption of digital avatars in Cyberspace gives ample opportunity for people to indulge in conduct which is not strictly ethical or moral and renders the task of fixing criminal and civil liability in Cyberspace difficult.

Identification and authentication in Cyberspace

10. Till now we have been relying heavily on paper based documents for all governmental and commercial transactions and communications and as we shift to electronic means of record keeping and electronic communication, a whole lot of legal as well as practical problems arise. Parties using electronic medium for transacting business need tamperproof electronic signatures to prevent electronic forgery since forgery and tampering with electronic records are perennial problems in Cyberspace. Electronic medium is ephemeral and any one with a rudimentary knowledge of programming can alter e-mail headers to fake the source of a message. Unless foolproof authentication is possible people will not transact business in Cyberspace. Viewed in this context the following questions derserve legal responses namely. Whether legally binding contract can be formed by exchange of electronic communication? What is the alternative for writing and signature in electronic medium? These issues have been addressed by means of the use of digital signatures.

Electronic Signatures, Digital Signatures and Biometric Tokens

11. Digital signature is a form of electronic signature but then every electronic signature is not a digital signature. Electronic signature may be a name or symbol affixed at the end of a message. All e-mail packages automatically affix user's name etc. in all the messages sent as a signature. This is meant to save valuable time and labour of typing out users name and address every time an e-mail is sent. Ordinary electronic signatures does not assure authenticity and integrity of the electronic record nor does it identify the sender. However digital signature ensures that a e-mail message was really sent by the person from whom the message appears to originate. In addition, a digital signature attests to the integrity of the contents of a message. Contrary to popular impression digital signature is not signature like manual signature where the user signs on any electronic format. That type of signature where a person signs with magnetic ink or special purpose pens are based on technology known as the signature dynamics and does not meet all types of requirements. In a closed circle like customers of a bank such a signature may be used because the specimen signature will be already available with the officer of the bank who has to clear the cheque or withdrawal request which enables him to verify the authenticity of the signature affixed on the cheque or the withdrawal form. It does not facilitate third party verification and does not enable total strangers to transact business without knowing each other because the other person has no means of knowing the signers original signature. If two persons not knowing each other were to interact and conclude transactions over the net it is essential for the other party to know whether the signature affixed is that of the party who has purported to have affixed it. The other techniques use biometric tokens which are based on the physiological characteristics of individual like retina scan, digital finger print etc. However these are all only techniques which ensures only those persons secure access whose biological features correspond to those biometric token contained already stored in the computer. It does not ensure the integrity of the electronic record. Further every

computer must have a digital camera or some special device which will be able to scan or read the biometric token of the user which will make the system very expensive and less popular since many people will not be able to afford the cost involved. At best biometric tokens are very useful in ATM counters where such a scheme can be implemented coupled with Personal Identification Number (PIN) but is not suited for generally doing commerce online. The only tested alternative which has been followed by many states in US and other parts of the world is Digital Signatures based on Public Key Infrastructure (PKI). Section 3 of the Information Technology Act, 2000 grants legal recognition to Digital Signatures based on PKI.

Digital Signature : How it works

12. Every Digital Signature is uniquely associated with the sender and there is no way to fake a signature by copying one signature from on document and attaching it to another, nor is it possible to alter the signed message in any way without the recipient immediately detecting the deception. This is made possible by means of Digital Signature Technology based on PKI which makes use of cryptography. Cryptography which is a branch of applied mathematics has multifold application in Cyberspace apart from digital signature. It is a software program generated by a Certifying Agency which can be preserved by a user in his hard disk. CD, floopy or in a smart card. A Digital signature consists of a key pair. A private key which only the user is supposed to know and a public key to which the private key corresponds. The public key is published in a repository which is like a public registry and is freely available to any one who wishes to make use of it to verify the message sent by holder of the private key corresponding top the public key. To digitally sign a electronic record the user will have to run the software programme over the message which will encrypt the message by means of the private key of the use. On encryption the message is reduced to an unintellible form and it transmitted along the net. Any person intercepting the encrypted message will not be in a position to make

head or tail of it. This ensures the integrity of the message. On receipt of the message the receiver will access the public key of the sender from the repository and apply it to the jumbled data which has arrived at his computer a process known as decryption. This will result in restoring the message to its original readable form. Any tampering of the message will immediately be indicated in the computer. It is true that nothing prevents any person who intercepts such a message encrypted with the private key of a sender from reading such a message because he can also access the public key of the sender form the repository. Encryption with the private key of the sender ensures only the integrity of the message namely that from the time it was encrypted till it was decrypted by the recipient, no tampering of the message has been place. To ensure confidentiality between the sender and the recipient, the message must in addition to being encrypted by the private key of the sender should also be encrypted by the public key of the recipient. Such message on receipt will be decrypted first by the recipient by the public key of the sender and thereafter by his own private key. Only then the original message will be displayed. If this course of double encryption is resorted to no person other than the recipient can decrypt the message and the message will be strictly confidential between the sender and the receiver. Thus it is possible to encrypt the same message by two different keys. Section 3 of the Information Technology Act, 2000 grants legal recognition to such Digital Signature based on PKI.

Admissibility in the Law of Evidence

13. Questions arise relating to admissibility of electronic records and transmissions in the law of evidence. Law presumes paper-based documents as proof of transactions. Difficulties arise when records are kept in the electronic forms. Law of Evidence has to ensure that electronic transmissions and electronic records will have the same value as paper-based documents and digital signature would be equally legal as a manual signature. The Indian Evidence Act, 1872 revolves around two types of evidence-oral evidence and documentary evidence. Documentary evidence is of two types – primary evidence and secondary

evidence. Primary evidence is where the original itself is available. Secondary evidence is where the contents of the original will have to be proved by leading in further evidence. Electronic records challenge this very assumption since in every electronic record is an original as well as a duplicate. In other words it is primary as well as secondary evidence at the same time. To get over this complex situation special provisions (Sections 65A and 65B) have been incorporated in the Indian Evidence Act 1872 through the Second Schedule of the Information Technology Act, 2000. The said sections provide for proving the contents of electronic records.

Copyright in Cyberspace

14. The question of how Copyright laws should be applied to Cyberspace poses complex and novel challenges. Copyright law protects original literary, dramatic, musical and artistic works, cinematographic films, broadcasts recordings. To what extent are website contents capable of being brought within these categories of protected work is not clear. Multi-media nature of the website blurs the above distinctions. A wide range of ordinary, accepted Internet activity like caching, framing, meta-tagging raise complex problems for Copyright Law. Further the liability of on-line providers for infringing activities transmitted through their facilities is yet to be clearly crystallized. The governing copyright statute in our country is the Copyright Act, 1957, Which requires comprehensive amendments to meet the challenges posed by digital works. Apart from the above musical copyrights pose special problems which require special mention.

MP3 Piracy in Cyberspace

15. There is music in the celestial sphere wrote Plato. We do not know whether there is any truth in Plato's assertion but definitely. Cyberspace is saturated with digital music. So popular is digital music that musical sites have over taken even sex related sites in terms of internet access. MP3 technology enables users to download. upload and store music in digital format. MP3 format is a compression system for music that compresses s song into a smaller size so it easy to transmit over the net without loss of audio

quality. This is a quantum leap in audio technology since as ordinary CD stores about 10 million bytes of data per minute of music on the CD and a three minute song will require 30 megabytes of data. To download a 30 megabyte data over telephone line would require hours. But using the MP3 format the same can be compressed into 3 megabytes of data without loss of audio quality and can easily be downloaded by any user over a telephone line connected to internet and played on his computer. It is now possible for individuals to create virtual libraries of all of their favorite tunes simply by downloading them from the Internet. Users can then enjoy these files in a variety of ways. They can listen to them on portable MP3 player or directly from their hard drives, they can send their files via e-mail to other music fans or they can upload their files to the internet for anyone to enjoy. And because the music is in digital form, each successive copy made of the sound file is of the same quality as its predecessor. The music industry and the artists feel threatened by this technology since it leads to rampant piracy. To police the Cyberspace for copyright violations is not going to easy. Copyright law has to strike a balance between the interests of the artists and the interests of the internet users.

Domain Name System

16. ***"What is in a name? That which we call a rose, by any other name would smell as sweet"*** exclaimed Juliet. But in Cyberspace everything revolves around what is called the Domain Name. Every resource on the Internet, such as a web page or a file of information has its own address known as the Uniform Resource Locator (URL) or a domain name which is part of this address which is assigned to each computer or service on the Internet. Development of browsers and search engines which make finding specific locations on the Internet relatively simple has given rise to new type of conflict of interests in Cyberspace. Most browsers now allow a surfer to find the web-site of a company by simple by guessing a Domain name. With the globalization and commercialization of the Internet, domain names have taken on a new significance as

business identifiers. Thus domain names based on intuition become valuable corporate assets. Domain names are now highly visible in real space as well showing up on television commercials, magazine advertisements and hoardings. In these new guises, Domain names conflict with trademarks and other traditional business identifiers. Two factors aggravate this problem. First, domain names are global and must be unique - a particular string of letters can link to only one site – while trademark may overlap in different industries or different geographical locations. Second it is common practice for may Internet users to guess at domain names.

17. Domain names are assigned by the Internet Corporation for Assigned Names and Numbers (ICANN) on behalf of the National Science Foundation of the U.S. on first come first served basis. First come first served basis was adopted because internet was started as a non commercial project and no commercial applications were foreseen. But soon when it became commercialized and a Domain acquired a business value disputes started arising in the naming process. First come first served principle his has led to cyber squatting which involves buying of domain names which have a close resemblance to a similar or identical recognizable trademark like movie titles, company names and products with a view to sell them to the trade mark holder at exorbitant prices. Since cyber squatting results in consumer fraud and public confusion impairing the economy by depriving the legitimate trade mark owners of substantial revenues and good will, many domain name disputes are arising in Cyberspace. Cyber squatting raises the question whether such practice should be dealt with as a crime or as a civil dispute. Though a Bill called the Anti-Cyber squatting Bill has been introduced in the Senate of the U.S. Public opinion is divided on this issue.

Cyber Crimes and Cyber War

18. Every Society prescribes code of conduct for its subjects. Standards of behaviour which each one of them should observe in their relations with each other. It also expresses its displeasure by prescribing punishment for deviant

behaviour. Till now no society has attained hundred percent compliance from its subjects. The battle between the good and evil goes on endlessly and Cyberspace affords another medium for criminals to spread their nefarious activities. Since e-commerce cannot flourish unless there is some payment mechanism to settle accounts and effect money transfers, borderless environment like Cyberspace offers a rich avenue for money laundering and other related financial frauds more and more criminals are migrating to Cyberspace. Further as we grow accustomed to depend more and more on computers and networks, survival of a nation can be easily threatened by dislocation of the information infrastructure by crippling the essential services like electricity and water supply, transportation and banking services. If these essential services are targeted then the havoc and damage caused to the society will be much more than those which can be caused by explosives. To combat this evil, nations are hurriedly revising their criminal laws to deal with cyber crimes. The Council of Europe is in the process of finalizing a Draft Convention on Cyber Crime which is likely to be adopted by U. S. also. Most of the offences referred to that Convention are taken care of by the Information Technology Act, 2000 although some by way of providing civil penalties. The Indian Penal Code provides for certain offences relating to documents. First Schedule to the Information Technology Act, 2000 makes amendments to the Indian Penal Code to amend those sections to take care of offences involving electronic records also. In particular section 464 which deals with forgery has been modified to take care of the offence of electronic forgery. What we are witnessing today as cybercrimes like cyber stalking and denial of service are all petty crimes compared to what is in store for us. The next world war it is said will be an information war and will be fought in Cyberspace. It is a strange paradox that internet which was developed as a technology to survive a nuclear war should itself become a battle ground of a greater war!

Privacy

19. Cryptography deals with converting messages into unintellible form (encryption) and retransforming them back into their original form (decryption). Cryptography employs algorithms which are also called keys. The basic purpose of cryptography is to maintain secrecy and confidentiality. Phreaking which gained popularity during the 1970s refers to the gaining of control of various portions of the telephone network with a view to create havoc and eavesdrop on private conversations. Since eavesdropping was one of the popular trend in phreaking IBM produced an encryption chip in 1974 called the Lucifer chip for warding of this evil. Lucifer was devised to maintain confidentiality in telephone conversations. The U.S. National Security Agency saw this as a threat to its intelligence gathering capabilities and wrested control from the National Science Foundation for setting standards about the encryption algorithms and about their strength. In that process it made the algorithm weaker than that IBM wanted it so that the device would be strong enough to be used by industry, but weak enough to allow National Security Agency to break it. Lucifer later evolved into the data Encryption Standard (DES), and algorithm to be used by government and industry to encrypt its important data and to encode confidential telephone calls. In 1993 a stronger algorithm called Skipjack, which relied on an 80-bit key, was developed by the National Security Agency. Skipjack's algorithm is being implemented through the Escrowed Encryption Standard, called the Clipper chip. Clipper chips are installed in telephones, faxes, and modems. Similar chips by the name of Capston are installed on the computer networks. In addition recently the Federal Bureau of Investigation unveiled a software program called Carnivore a diagnostic tool to intercept messages on the internet which sniffs network packets for predetermined filter set of programs. While Clipper and Capston were meant to safeguard privacy of individuals with the state maintaining its right to invade the privacy in public interest by insisting on keeping the key escrow which will enable its agencies to decrypt messages.

Carnivore on the other hand is an outright surveillance tool to spy on individuals. The use of these techniques is rigidly controlled by the legal process in U.S. since they threaten the privacy of individuals. It is here one of the bitter battles are going to be fought between state agencies entrusted with maintaining law and order and the proponents of right of privacy.

Dream and reality

20. Cyberspace is the realization of the dreams and vision of many. Creativity always comes from women. One of the inspiring personalities behind the Babbage's analytical engine which is the precurson of the modern computer is Lady Ada Lovelace Byron. She predicted in 1863 that machines will compose complex music, produce graphics and would be used for practical and scientific purposes. That prediction has come true. Tim Berners-Lee wanted a common information space in which people can communicate and share information freely. World Wide Web is the realization of that dream. He conceived Cyberspace as an abstract place where knowledge based economy happens. He also wanted web to become a realistic mirror of the ways in which we played and worked and socialized. He has predicted that the web will open up new dreams of business opportunities and turn bureaucracy over to machines and let people get on with creativity. It will help people to work together more effectively remove misunderstanding and bring about peace and harmony on a global scale. But according to him we can only do these things if we learn to use it wisely and think carefully about both the technology and the laws we make or change around it. Technology has always threatened to destroy Man if not controlled properly. Neuromancer describes the evils which a society must suffer if it willingly allows itself to be directly controlled by technology, 2001: A Space Odyssey also conveys the same message. HAL in 2001 is, in fact, the ultimate tool, he is so advanced that in conversation, it is practically impossible to tell that he a machine and not a human being. The similarly of man to his tools has reached its peak in HAL. a tool similar to a man, But, like all tools, HAL proved to be as dangerious

as he was useful. The moral of the story is that if we create incredible technologies we should not use them for evil and material gain, but for improving the lot of mankind. We can do that only if we do not become slaves of technology. Technology is a moral and value neutral. It is for us to use them intelligently and wisely for the benefit of mankind.

Conclusion

21. Greatest threat to mankind today emanates not form nuclear weapons, terrorism of from the spread of AIDSs, but from ***human greed, hypocrisy and misunderstanding***. When people have free access to each other, racial, language, cultural and religious barriers are bound to breakdown. If addressed properly Cyberspace will facilitate this process and usher in global peace and harmony. In the above scheme of things where does Indian Stand? Perhaps nowhere in the history of mankind. India is better positioned than today to take advantage of a historic revolution namely the digital revolution. Today, knowledge is capital and we have plenty of it. We are all knowledge capitalists. Cyberspace affords us opportunities for accelerated integration into global economy. It affords us vast opportunities for accessing new international markets at low cost and with minimum capital investment. It can provide avenues for our unemployed youth to earn their livelihood. If can lead to empowerment of women. This not a far fetched dream of an idealist but a prediction of a visionary. Consider the following. The language of internet today is English. But technology is evolving in such a way that people will be able to exchange ideas with each other thought they may communicate in different languages over internet with each other. When different computers were connected to each other it was difficult to forsee how different machines can interact with each other without a common operating system. But client-server technology has made this possible. Similarly people will be able to break the language barriers and communicate freely across the globe without the need for knowing the language of the other person. Once this happens we will be in a position to capitalize our knowledge base in a grand scale. This will be possible due to software programs that

are on the anvil. Our captains of Info Tech industry have proved that they are capable of making forays into the global economy. The Information Technology Act, 2000 enacted in the budget session of Parliament and brought into force recently is first in a series of legislations which are required to deal with issues relating to Cyberspace. The Act inter alia also seeks to usher in electronic governance by permitting grant of permissions, licences etc. by Government agencies and the filing applications etc. by electronic means with the Government agencies by individuals thus making the life of the citizens interaction with the Govermental agencies hassle free. Above all it grants legal sancity to Electronic Gazette which apart from increasing legal literacy will go a long way in providing easy access to citizens, rules, notifications etc. which have profound effect upon their daily lives. ***In short the Act is a millennium gift given by Parliament to the people of India. It is a great tribute to the Members of Parliament as a whole, for rising above party considerations and approving the legislation unanimously and speedily. Ours is an ancient civilization. We have suffered enough. Now our time has come. For historical reasons we might have missed the industrial revolution but surely our younger generation has not missed this digital revolution which is sweeping across the world. Pride of place must be accorded to our young software engineers for keeping the flag of India flying high. The enactment of the Information Technology Act, 2000 sends strong signals to the world that we are a digital force to be reckoned with. It also sends a strong message to the world that Indians are coming and are coming in a big way and they are going to conquer Cyberspace!***

The WIPO Domain Name Dispute Resolution Process: An Effective Alternative Mechanism

*Shyamkrishna Balganesh**
*Neelanjan Maitra**

Introduction

With the emergence of the Internet as the largest global market, the use and misuse of intellectual property in electronic transactions has assumed phenomenal proportions. Among them, domain name disputes still remain one of the most serious complications to have arisen with regard to the application of traditional trademark law to the Internet.

At its simplest level, the domain name problem centers around the use of registered and well-known marks in the domain name of a web-site, used to identify and locate a web-page. A domain name is part of the address that is assigned to each computer or service on the Internet[1]. The problem essentially arises when a registered or well known mark is assigned as part of this address to a party which is not the proprietor of this mark, since allotment of domain names is done on a first-come first-served basis. The application of traditional trademark law in resolving this problem has presented courts all over the world with several problems, establishing jurisdiction in light of the global nature of the Internet, applicability of law and the like[2].

---

* III year. BA, LL.B (Hons.) National Law School of India University, Bangalore.

[1] Charlotte Waelde, "Domain names and Trade marks : What's in a name?". Lilian Edwards and Charlotte Waelde, eds. *Law & the Internet : regulating cyberspace*, 1st edition, Hart Publishing, Oxford, 1997, pp. 45-66.

[2] For more details see. Margaret Nco, *Taking the Mystique Off Domain Names*, at (visited on 3rd February, 1999) <http;/home1. pacific, net,sg/~jhmk/article 14 html>: Todd Gascon, *Arts & the Law : A Primer on Domain names and Trademarks*, at (visited on 15th June, 1999)<http.//www.artsfusion.com/1999/april/artsandlaw.html> Pasquale A. Razzano and Bruce M. Wexler, "US Battles International Coalition Over New Domain Name System", *IP Worldwide*, May/June, 1998, p.13': Jonathon E. Moskin, "Domain Name "Reforms" Will Inflame Internet Problems". IP Worldwide July/August 1998, p.3.

Based on a suggestion given by the Government of the United States of America and with the approval of all its member states, the World Intellectual Property Organisation (WIPO) undertook a series of consultations since July, 1998 and based on the same made recommendations to the Internet Corporation for Assigned Names and Numbers (ICANN), the organisation which administers domain names globally. The final draft of these recommendations constitutes the *Final Report of the WIPO Internet Domain Name Process*[3].

As a result of these consultations, the WIPO came up with the Uniform Domain Name Dispute Resolution Policy, which was subsequently approved by the ICANN on October 24, 1999. This policy provides an alternate arbitration mechanism for the settlement of domain name disputes. In the Course of this brief paper, an attempt is made to outline some of the characteristic features of this process and where it attempts to fill the gaps produced by the application of traditional dispute settlement processes to the resolution of domain name disputes globally.

Of Domain Names and Trademarks in General

Before getting into an analysis of the WIPO process, this part provides a very brief overview of the concept of domain names and the controversy presented by their unregulated registration.

The purpose of a domain name is to identify the computer, which has been accessed on the Internet, which at the basis level is no more than a collection of computers connected through telephonic networks to communicate with each other[4]. A domain name consists of alphanumeric characters separated by dots[5]. The first group of characters represents the name of the enterprise or the brand name/trading name associated with the enterprise called the 'Second Level Domain'. This is followed by a "Top Level Domain" or a TLD,

---

[3] *The Management of Internet Names and Addresses : Intellectual Property Issues* – Final Report of theWIPO Internet Domain Name Process, April 30, 1999.

[4] *See, British Telecommunications v. One In. A Million*, [1998] 4 All. ER 476, 480.

[5] Such as *sony.com.Microsoft.com* and the like.

which identifies the nature of the enterprise[6] and sometimes the geographical area where the enterprises is present[7].

Any alphanumeric characters or words can be included in the Second Level Domain. The problem arises when a registered mark or a well known mark is registered as part of the domain name by a party not owning the proprietary rights over the mark in question. Matters are further complicated by the fact that trademark law is municipal and country-specific whereas the Internet is truly global and boundary–less.

The domain name conflict has confronted legal systems in all parts of the world. Not only technologically advanced nations of the west, but developing nations like India too have had to face this problem[8]. This complicates the issue further, because while developed nations may have foreseen such problems and have enacted technology specific legislation, developing nations like India are forced to apply existing laws to the Internet, with considerably less fruition.

The uniform Domain Name Dispute Resolution Policy[9]

As a part of its final report, the WIPO introduced the Uniform Domain Name Dispute Resolution Policy[10]. The policy essentially sets out the legal framework to be adhered to in the event of a dispute about the assignment of domain names, between the assignee and any third party. The policy, after being accepted by the ICANN , was ratified by all the ICANN-accredited registrars, in charge of registering domain names locally and coordinating through the ICANN.

The policy is mainly in the form of an agreement between the assignee of a domain name and the registrar, whereby the assignee

---

[6] Called the generic, TLD. These are *.com* for international commercial organizations,. *.edu* for educational establishment,.*gov* for governmental organizations and *.org* for other organizations.

[7] Called the country code TLD such as. *.in* for India,.*uk* for the UK and *.au* for Australia.

[8] *See. Yahoo! Inc.v. Akash Arora*, [1999] IPLR 196; also the unreported judgement in *Titan Industries v. Prashant Kooapati*, (Delhi High Court).

[9] Hereinafter referred to as "the policy".

[10] *Uniform Domain Name Dispute Resolution Policy*, at (visited on 8th March, 2000) >http:/WWW.icann.org/udrp-policy-24oct99.htm>.

agrees to abide by certain specified rules and regulations in the event of any dispute as to the assignment of the name. The policy has application not only in agreements entered into, after 24th October, 1999 but also in previous agreements by virtue of the fact that in most agreements entered into by ICANN-accredited registrars, there exists a clause whereby the assignee agrees to abide by any dispute resolution policy adopted by the registrar. In effect therefore, the policy has a retrospective application too.

The operative part of the policy, with regard to the dispute settlement process is to be found in paragraph 4, which relates to mandatory administrative proceeding. The paragraph provides that the entire proceeding is to be conducted before an administrative dispute resolution service provider to be selected from a list of such providers accredited by the ICANN. Paragraph 4 goes on to provide that the assignee is required to submit to the mandatory administrative proceeding if a complaint is filed by a third party alleging:

(a) that the domain name assigned is confusingly similar or identical to a trade or service mark in which the complainant has rights;
(b) that the assignee has no legitimate interest or rights in the domain name;
(c) that the assignee has registered and used the domain name in bad faith.

It is important to note that all three requirements need to be alleged by the complainant[11].

These form the substantive in which a third party can file a complaint about the assignment of the domain name. It will be seen that the requirements are quite different from a mere trademark infringement allegation. Whereas generally in traditional trademark confusion cases[12], it is essential that the use of the mark must be in relation to similar goods or services, in the present scenario no such restriction is placed. It may therefore be argued that a component of

[11] Paragraph 4, "... In the administrative proceedings, the complainant must prove that each of these three elements are present."
[12] For instance under the Trade and Merchandise Marks Act, 1958.

the doctrine of trademark dilution is also incorporated into paragraph 4. However, traditional dilution law requires that the mark alleged to have been infringed must be registered or a well known mark. No such requirement in found in paragraph 4. The scope therefore is wider than in traditional trademark infringement.

Coming to the second requirement, it is seen that the onus to prove that the respondent has no legitimate interest in the usage of the mark is placed on the complainant. The phrase 'legitimate interest or rights in the domain name', have been accorded a specific meaning in the policy. What exactly it constitutes is to be found in paragraph 4 (c) of the policy. The three conditions when the respondent can be said to have a legitimate interest or right in the domain name in question are:

1. Where, prior to the dispute the respondent (i.e. the defendant) has used or has made preparation to use the domain name corresponding to the one in dispute in connection with a *bona fide offering of goods and services*[13]. What exactly would go into making an offering of goods and services *bona fide*. This, it is submitted introduces a subjective element into the adjudication process and is to be ascertained based on the specific facts and circumstances of each case.
2. Where the respondent has been commonly known by the domain name in question though he has acquired no trademark or service mark in the same[14]. This again introduces a good deal of ambiguity into the entire process. Fundamentally, how is one to ascertain whether the respondent has been commonly known by a particular name. The problem may be further complicated by the cross-border applicability of the policy. Thus, the respondent maybe well known by the name in a particular nation, whereas the applicant may have registered his mark in another.
3. Where the respondent has been making a legitimate non-commercial or fair use of the domain name without any intention of commercial gain or to misleadingly divert

[13] *See*, paragraph 4(c) (i).
[14] Paragraph 4 (c) (ii).

consumers or to tarnish the trade or service mark[15]. By making express reference to the term 'tarnish', we see that the policy recognizes the concept of trademark dilution referred to earlier. Once again, the question over what exactly constitutes a *non-commercial fair use* has to be determined on the facts of each specific case.

The third requirement is that the respondent should have not only registered the domain name in bad faith, but he should have also made use of the same in bad faith. Mere registration or mere use is insufficient to constitute an action under paragraph 4. Paragraph 4 (b) contain a list of indicators to ascertain when a person is said to have registered the domain name *and used* it in bad faith. They are[16]:

- Traditional *cybersquatting*, where the respondent registers the name to sell it or transfer it to the trademark holder or his competitor for a price.

---

[15] Paragraph 4 (c) (iii)

[16] Paragraph 4 (b)

"Evidence of Registration and Use in Bad Faith. For the purposes of Paragraph 4(a)(iii), the following circumstances, in particular but without limitation, if found by the Panel to be present, shall be evidence of the registration and use of domain name in bad faith:

(i) circumstances indicating that you have registered or you have acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of your documented out-of-pocket costs directly related to the domain name; or

(ii) you have registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that you have engaged in a pattern of such conduct; or

(iii) you have registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name , you have intentionally attempted to attract, for commercial gain, Internet users to you web-site or other on-line location, by creating a likelihood of confusion with the complainant's mark as to the source, sponsorship affiliation, or endorsement of your web-site or location or of a product or service on your web-site or location.

- Where it has been registered to prevent the trademark holder from registering such a domain name himself, *provided the respondent has engaged in a pattern or such conduct.* Once, again a question, which remains unanswered, is *what constitutes a pattern of such conduct?*
- Where it has been registered mainly to disrupt the business of a competitor.
- Where it has been registered to attract users to the site by *creating a likelihood of confusion* with the applicant's mark.

These three conditions contained in paragraph 4 (c) have to be mandatorily satisfied as conditions precedent to the entertainment of a proceeding by the panel. A further point to be noted is that the policy can be administered not only by the WIPO Arbitration Centre but also by other provides who have accepted the policy upon its adoption by the ICANN[17].

Coming now to a more fundamental issue involving the entire adjudicatory framework, namely, that of the remedies available to the adjudicatory authority, i.e., the provider. Under the policy, only two remedies are available to the provider[18] :

- *Cancellation* of the domain name registered;
- Ordering the *transfer* of the domain name in favour of the complainant (i.e., the person who has a ligitimate interest or right in the name or who has a trade or service mark to that effect).

In practical terms therefore the process is not a substitute for an actual civil proceedings in a court, where the court may in addition also award damages or grant an injunction in favour of the complainant. The powers given to the adjudicatory authorities are therefore considerably limited. As a result, the policy expressly contemplates that in a majority of cases, either party may approach a court of competent jurisdiction on the same issue.

---

[17] *See*. Paragraph 4 (d)
[18] *See*. Paragraph 4 (i)

Thus, the policy provides that once a decision has been reached by the panel appointed by the adjudicatory authority, the authority will wait for ten days before implementing the decision of the authority. During this period if the authority receives official documentation that either party has approached a court, then it will not implement the decision until the court has adjudicated on the matter or until both parties reach a settlement[19]. Thus, the jurisdiction of a competent civil court is not ousted. Since the decision of the arbitrator may be in addition to the remedy prescribed by the court, the remedies of damages and specific relief are not completely ruled out. One can therefore look at the WIPO process as a regulatory mechanism, more administrative than actually adjudicatory.

Finally, the policy also prohibits a change in the registrar [20] of the domain name in question or a transfer of the domain name in question during the pendency of the prescribed arbitration proceeding or for a period of 15 days thereafter . In addition, it also prescribes such actions when any dispute relating to the domain name is pending before any arbitration panel or a court unless the transferee[21] or in the case of change in the registrar[22], the registrant agrees to be bound by the decision of such an arbitration panel or court. In cases, where such a change in registrars actually occurs, the policy clearly provides that the registrant is bound by the terms and conditions relating to dispute resolution as provided by the earlier registrar[23]. This is meant to prevent a situation where, a respondent seeks to take advantage of the situation by shifting his registration to a registrar where the policy is not yet in force. The registrar in question at the time when the action is initiated is taken into consideration.

---

[19] Paragraph 4(k)

[20] This is a case where a person obtains a domain name registration with one registrar and thereafter when a proceeding is initiated against him by an applicant, he transfers the registration to another registrar.

[21] Paragraph 8 (a) deals with transfers during the pendency of the dispute.

[22] Paragraph 8 (b) deals with changes made to the Register of the Provides during the dispute.

[23] *Id.*

The Procedure

In the previous part, we have seen the substantive law relating to the policy regarding the arbitration. It is equally important to understand the exact procedure to be followed right through the arbitration process and analyse the reasonableness of the same.[24]

The entire procedure commences when the provider receives the complaint from the complainant[25]. Upon receipt of the same the provider is to take reasonable steps to ensure actual notice of the complaint to the respondent. Actual notice to the respondent is said to have been achieved when the provider achieves the same or takes certain measures to ensure actual notice such as putting the complaint into postal mail to the respondent of sending the same electronically to the respondent[26].

Upon receipt of the complainant the provider is under an obligation to ensure that the complaint has compiled with all the modalities as laid down in the rules. In the event the provider finds the complaint to be deficient, the provider must notify the complainant and the respondent of the deficiency. The complainant then has 5 days within which to make the required changes. If he does not do so within the prescribed time, the complaint is deemed to have been withdrawn[27]. Once the provider finds the complaint to be in order and accepts the same, the administrative proceeding is deemed to have been initiated[28].

Once the complaint has been accepted and notice of the same has been sent to the respondent, the respondent can filed a response to the same. The response too, like the complaint must comply with certain procedural requirements[29]. The respondent is given a period of 20 days to file the response. If the respondent fails to file a response and there are not exceptional circumstances, which require a

---

[24] The rules are governed by the Rules for Uniform Domain Dispute Resolution Policy, available at http://www.Icann.org/udrp/udrp-rules-24oct99.htm.>.

[25] *See.* Rule 3.

[26] Rule 2, Rule 2 also contains an elaborate list of guidelines the complaint has to comply with in order to be ascertained as valid and acceptable.

[27] Rule 4

[28] Rule 4 (d)

[29] Rule 5

response, the adjudicatory panel can proceed based on the complaint alone.[30] Here, again the ambiguity returns. What exactly constitute exceptional circumstances ? This is to be decided by the panel based on the facts of each case.

Once these procedures have been complied with, the provider will appoint a panel consisting either of a single member or of three members to decide the dispute[31]. Upon such constitution, the panel appointed has to assure the provider and the parties of its impartiality and independence in the proceeding[32].

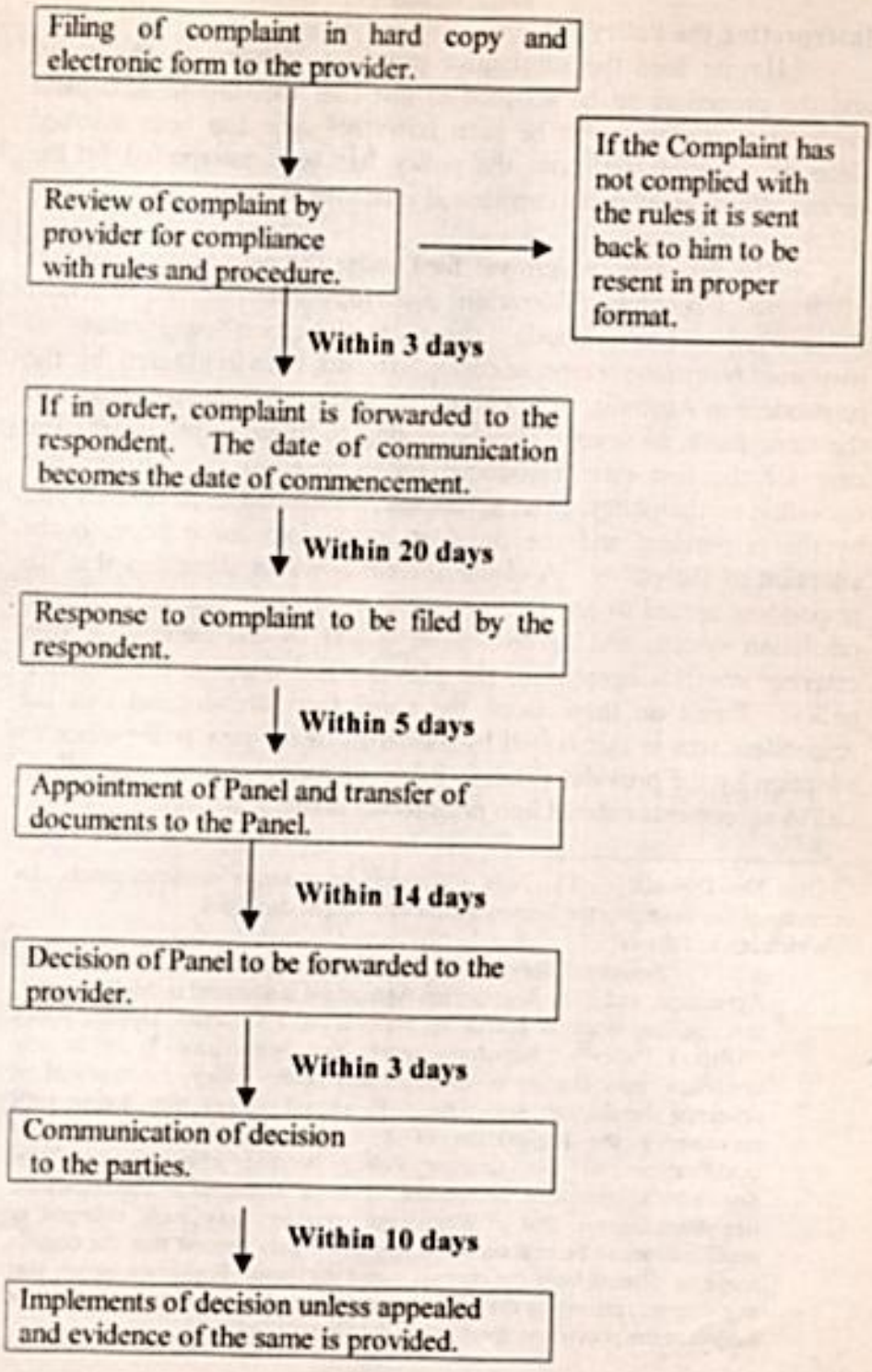
The panel is supposed to reach a decision within 14 days from its constitution and forward the same to the provider [33]. The provider upon receipt of the decision is to communicate the same to the parties within 3 days[34] . During the pendency of the proceeding if the parties effect a settlement or if for any reason it becomes impossible or unfeasible to continue the proceedings the panel may terminate the same. Here, again the panel is given complete discretion to decide when continuance of the proceeding has become impossible or unnecessary[35]. An aggrieved party however can raise an objection with the panel on its decision.

If during the pendency of the proceedings before the panel, either party files a suit in a court of competent jurisdiction relating the domain name in dispute, the party is to communicate the same to the panel and then it is left to the complete discretion of the panel to decide whether to suspend, terminate or continue the proceedings[36].

The entire process is extremely efficient and streamlined in theory. The procedure for resolution of the dispute is considerably elaborate and can cover a wide range of circumstances. The process as a whole can be represented schematically as follows;

---

[30] Rule 5 (e)
[31] Rule 6.
[32] Rule 7.
[33] Rule 15
[34] Rule 16.
[35] Rule 17
[36] Rule 18.


Filing of complaint in hard copy and electronic form to the provider.
Review of complaint by provider for compliance with rules and procedure.
If the Complaint has not complied with the rules it is sent back to him to be resent in proper format.
Within 3 days
If in order, complaint is forwarded to the respondent. The date of communication becomes the date of commencement.
Within 20 days
Response to complaint to be filed by the respondent.
Within 5 days
Appointment of Panel and transfer of documents to the Panel.
Within 14 days
Decision of Panel to be forwarded to the provider.
Within 3 days
Communication of decision to the parties.
Within 10 days
Implements of decision unless appealed and evidence of the same is provided.

Interpreting the Policy

Having seen the substantive provisions relating to the policy and the procedure to be adopted in invoking the dispute settlement mechanism, it remains to be seen how the same has been invoked since its adoption and how the policy has been interpreted by the various adjudicatory panel constituted under the scheme.

The first case, which was filed under the new policy, was that of *World Wrestling Federation Entertainment Inc. vs. Michael Bosman*[37]. The domain name in question was that of *www.worldwrestlingfederation.com*. It had been registered by the respondent in Australia. The complainant was the trademark holder of the same name, in several classes relating to different products. The case for the first time introduced the concept of the retrospective operation of the policy. The agreement, which had been entered into by the respondent and the provider, came into force prior to the adoption of the policy. A clause therein however stipulated that the respondent agreed to any changes made by the provider in its dispute resolution system and agreed to be bound by the same [38]. After entering into this agreement, the provider had adopted the UDNDR policy. Based on these facts, the panel therefore decided that the respondent was in fact bound by the terms of the new policy since its adoption by the provider result in it being given a retrospective effect, i.e., to agreements entered into prior to the actual adoption.

---

[37] Case No. D99-0001. This was a decision by a single member panel. Its importance lies in setting the framework for subsequent decisions.

[38] Which ran as follows"

> "Registrant agrees, as a condition to submitting this Registration Agreement, and if the Registration Agreement is accepted by Melbournel T, that the Registrant is bound by Melbournel T's current Dispute policy ("Dispute Policy") Registrant agrees that Melbournel T, in its sole discretion, may change or modify the Dispute Policy, incorporated by reference herein, at any time. Registrant agrees that Registrant's maintaining the registration of a domain name after changes or modifications to the Dispute Policy become effective constitutes Registrant's continued acceptance of these changes or modifications. Registrant agrees that if Registrant considers any such changes or modifications to be unacceptable. Registrant may request that the domain name be deleted from the domain name database, Registrant agrees that any dispute relating to the registration or use of its domain name will be subject to the provisions specified in the Dispute Policy"

Upon filing of the complaint by the complainant and dispatching of the notice by the provider, the respondent failed to reply and the case was commenced notwithstanding the default by the respondent When the panel was deciding on the issue it received notice from the parties that they were in the process of negotiating a settlement. No formal settlement was received by the panel and it therefore felt obligated to provide a timely decision. One of the fundamental issues that arose for consideration was whether there was sufficient evidence of the respondent not only *registering* the name in bad faith but also *using* the same in bad faith[39]. In this context, the panel referred to paragraph 4 (b) (i) of the policy and noted the phrase used there indicated that the section provided instances where the respondent could be said to have *registered and used* the domain name in bad faith. One such requirement provided therein is the traditional case of cyber-squatting where the respondent registers the name and attempts to sell the same to the complainant or a competitor of the complainant for a consideration.

An examination of the facts revealed that upon registration the respondent had contacted the complainants and had offered to sell them the name for $ 1000[40]. The Court therefore concluded that it was a case of traditional *cybersquatting* and amounted to a case of registration and use in bad faith by the respondent. Accordingly the

---

[39] In reaching this decision the court relied on the legislative history behind the framing of the policy and statements made during the process of drafting the same.

> "These comments point out that cybersquatters often register names in bulk, do not use them, yet without use the streamlined dispute – resolution procedure is not available. While that argument appears to have merit on initial impression, it would involve a change in the policy adopted by the Board. The WIPO report, the DNSO recommendation, and the registrars-group recommendation all required both registration and use in bad faith before the streamlined procedure would be invoked. Staff recommends that this requirement not be changed without study and recommendation by the DNSO. " *Second Staff Report on Implementation Documents for the Uniform Dispute Resolution Policy, submitted for Board meeting of October 24, 1999, para 4,5 a.*

[40] The court also reviewed the statement made by the respondent to the complaint in his correspondence that cyber-squatting cases."..... typically accomplish very little and end up costing the companies thousands of dollars in legal fees, wasted time and energy."

court ruled in favour of the complainants within the 45-day period[41] and ordered the transfer of the domain name in favour of the complainants.

This was the first case that actually interpreted the terms of the policy in its implementation. Since then, the procedure has been used extensively by enterprises and individuals from several nations. In *Robert Ellenbogen v. Mike Pearson*[42], a curious situation arose. Here, the defendant when given notice of the proceedings, replied stating that he had no connection with the domain name in question and was seeking to have his name dissociated from the domain name. Nevertheless, the panels held that the act of seeking to dissociate himself was itself evidence of use in bad faith and accordingly ordered the retransfer of the name.

In a majority of cases, the panels constituted under the policy have found evidence of registration and use in bad faith based solely on an offer by the defendants to sell the domain name to the plaintiff at an extraordinary high cost. This was the situation in the *Mary-Lynn Mondich v. American Vintage Biscuits*[43].

There have also been several cases where the panels have failed to find a legitimate interest with the plaintiff to transfer ownership of the domain name in dispute. In *Telaxis Communications v. William Minkle*[44], the defendant was a real estate businessman who registered a domain name. At the time of registration, the plaintiff had no interests in the name in question. Subsequently, the plaintiff company obtained a trademark over the name which had been used in the domain name and initiated proceedings under the policy was re-transferring of the domain name to them. The panel held that it was satisfied that the defendant had a legitimate interest in the domain

---

[41] The complaint was received on 2nd December, 1999 and the decision of the panel was communicated to the provider by 14th January, 2000

[42] Case No. D 00-0001.

[43] Case No. D 00-0004, See also, *Talk City Inc. v. Michael Robertson.* Case No. D 2000-0009; *Ronson. plc. v. Unimetal, Sanayi*, D 2000-0011.

[44] Case No. D 2000-0005, Similarly, in *Digitronics Inventioneering Corporation v. @Six Net Registered.* Case No. D 2000-0008, the penal refused to make an order since it found that the defendant had a legitimate interest in the domain name registered.

name and therefore, though there was confusing similarity between the marks, no order of transfer could be granted. In *Adaptive Molecular Technologies vs. Priscilla Woodward*[45], the defendants were 'stocking distributors'of a product of the plaintiffs in which the latter had a registered trademark. The defendants obtained a domain name registration of the name and informed the plaintiff company. The news met with a positive response. Subsequently, when relations soured between the companies, the plaintiff company sought to recover the registration of the domain name. The panel rightly concluded that the defendant had not registered the name in bad faith and in fact had a legitimate interest in the name. Accordingly, it refused to order a transfer of the registration.

Another interesting set of cases involves organizations that register domain names of well-known trademarks and sell the domain names back to the owners of the marks at high rates *on a commercial basis*. In such cases too, the policy has been used to transfer the domain names back to the actual owners of the marks upon a finding that the registration and use was in bad faith[46].

Ever since its introduction, the policy has therefore found widespread use and acceptance. It has been applied in a wide variety of fact situations, indicating its inherent flexibility and adaptability. Aggrieved parties from different part of the world have sough to use the mechanism, indicating its effectiveness in dealing with the problem of jurisdiction[47].

Conclusion

To conclude, the new WIPO DND Policy has over the past few months since its inception proved to be efficacious both substantively and procedurally. The problem of resolving domain name disputes involves issues of jurisdiction, nature of liability, enforcement and the like. The new policy for the first time provides a comprehensive response to the problem. It recognises that since the source of the problem is the Internet, the solution ought to lie in a mechanism that

---

[45] Case No. D 2000-0006.

[46] *See. Stell D'oro Biscuit Co.v. The patron Group*, Case No. D 2000-0012; *Nabisco Brands v. The Patron Group* , D 2000-0032.

[47] In 2000 alone more than 1600 complaints have been filed. Out of them 32 have involved Indian complainants.

makes optimal use of the same medium. The online procedure is representative of this.

Its effectiveness more than anything else is evidenced by the number of cases that have been filed ever since its inception. In short the new policy provides a one-stop solution to the entire domain name dispute problem and transcends national boundaries in its enforcement; something no other policy has been able to achieve successfully in the context of the Internet.

<:> <:> <:>

- ***"When you make a difference in someone else's life your life will be forever different."***

-N.K. Donnoy

FROM THE PEN OF DIRECTOR

Learning from past shapes the future. Ignoring the 'just' may create anarchy. India the great country, when became Independent many pledges were taken. On the eve of attainment of Independence Pt. Jawahar Lal Nehru has said that " we end today a period of ill fortune and India discovers herself again. The achievement we celebrate today is but a step, an opening of opportunity, to the greater triumphs and achievement that awaits us. Are we brave enough and wise enough to grasp this opportunity and accept the challenge of future". Has India discovered itself again? The answer perhaps lies in the 50 years history of Independent India. Have we been capable to effectively and rationally explore and utilize our resources? Apart from counting our achievements it is time for introspection also. As far as judiciary is concerned no doubt it has ventured new areas with the changing needs and aspirations of the people but at the same time the whole system of justice delivery system has been questioned due to delay in disposal/decision of cases and docket explosion.

A system is assessed by the results it delivers and the results depend upon the personnel who manage it. Judges are viewed with a different eye; they are expected to be more virtuous and rightly so. About the most important judicial qualities it is said that they are; quality and competence and temperament & character & diligence. Sense of fear and favour trembles the soul of justice. Knowledge with virtue adds wisdom. Virtuous thorough knowledge with dedication to duty without fear and favour results in a just action, which adds glory to the system.

The Saintly qualities which a judge is expected to practice and profess in itself denies deviation from virtue. Knowledge, virtue, wisdom, dedication to duty and purity in action coupled with compassion makes him complete and the demands of materialist body for sense gratification does not disturb him. Truth is nothing more nothing less but truth. It is well said that everything can be sacrificed for truth but truth cannot be sacrificed for anything. Action springs from thought therefore, purity of thought is a condition precedent for

purity in action. Corruption in any of its form pollutes whole of it. Morality cannot be sermonized but it is a matter of action.

In this age of information technology when everything is changing fast computer have revolutionized the way of living in general. Distances are reduced, new trends and threats have emerged. With changes economic reforms have got new dimensions. The scopes of the Intellectual Property Rights have been widened. Newer disciplines of law have to be dealt with all promptitudes. On 28 August, 2000 while inaugurating the refresher training programme for Civil Judges (Senior Division) Hon'ble Mr. Justice S.K. Sen, the Chief Justice of Allahabad High Court emphasized that thorough knowledge of the procedural laws and basics is the need of the hour for expeditious and just decision of cases and to control the working of the court and further expressed that money is not everything by citing an example of hockey that in by-gone days India was champion of hockey though very less amount was meant for sports in those days whereas, presently inspite of huge expenditure on sports still India is struggling to maintain its identity in the field of hockey. His Lordship has on that occasion impressed upon the officers to discharge their duties fearlessly and without favour.

To prepare the Judges of future the Institute have been endeavoring to strive towards excellence and imparting training in such a manner so that high values and virtues may also be imbibed by the trainees. During the period of last four months the following training programmes were conducted by the Institute.

Sl. No.	Details of Training	Duration	No. of trainees participated in the training
1	Computer Training Programme for Judicial Officers	24.07.2000 to 29.07.2000	19
2	Computer Training Programme for Judicial Officers	31.07.2000 to 05.08.2000	20

3	Computer Training Programme for Judicial Officers	07.08.2000 to 11.08.2000	24
4	Computer Training Programme for Judicial Officers	14.08.2000 to 19.08.2000	15
5	Computer Training Programme for Judicial Officers	21.08.2000 to 26.08.2000	10
6	Refresher Training Programme for Civil Judges (Senior Division) / CJMs / ACJMs	25.08.2000 to 07.09.2000	28
7	Computer Training Programme for Judicial Officers	28.08.2000 to 02.09.2000	16
8	Computer Training Programme for Judicial Officers	04.09.2000 to 08.09.2000	16
9	Training Programme on Law Subjects Officers of Combined State Services	11.09.2000 to 15.09.2000	29
10	Computer Training Programme for Judicial Officers	11.09.2000 to 16.09.2000	12
11	Computer Training Programme for Judicial Officers	18.09.2000 to 23.09.2000	16
12	Refresher Training Programme for Addl. District & Sessions Judges	10.10.2000 to 21.10.2000	31
13	Training Programme on Law Subjects for Jail Officers	13.11.2000 to 17.11.2000	28
14	Computer Training Programme for Judicial Officers	27.11.2000 to 02.12.2000	14

15	Computer Training Programme for Judicial Officers	04.12.2000 to 08.12.2000	09
16	Special Training Programme on "Compensation Laws" (Land Acquisition Act and MV Act) for Addl. District and Sessions Judges.	04.12.2000 to 08.12.2000	22
17	Special Training Programme on "Criminal Law in practice" for Addl. District and Sessions Judges.	11.12.2000 to 15.12.2000	26
18	Computer Training Programme for Judicial Officers	11.12.2000 to 16.12.2000	12
19	Training Programme on "Legal Procedure and practice and contractual matters" The officers of Indian Defence Accounts Services.	18.12.2000 to 22.12.2000	24
20	Training Programme on "Legal Services Authority Act, 1987" for The "Secretaries" of the District Legal Authority, U.P.	19.12.200 to 21.12.2000	25

For the year 2001 the Institute proposes the following training programmes:

DURATION	NAME OF TRAINING/ WORKSHOPS AND CONFERENCES
06.01.2001 to 18.01.2001	National Level Training Programme on Cyber Law and Cyber Crimes for the Judicial Officers.

22.01.2001 to 27.01.2001	Sansitisation Programme on Human Rights 1st Phase in collaboration with NHRC, for the Presiding Officers of Human Rights Protection Courts
22.01.2001 to 27.01.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
30.01.2001 to 03.02.2001	Sansitisation Programme on Human Rights 2nd Phase in collaboration with NHRC, for the Presiding Officers of Human Rights Protection Courts.
12.02.2001 to 17.02.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
13.02.2001 to 24.02.2001	Refresher Training Programme for Addl. District and Sessions Judges
19.02.2001 to 24.02.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
26.02.2001 to 03.03.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
27.02.2001 to 01.03.2001	Training Programme for the Secretaries of District Legal Services Authority, U.P.

19.03.2001 to 24.03.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
16.04.2001 to 26.04.2001	Refresher Training Programme for Civil Judges (Senior Division)
16.04.2001 to 21.04.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
23.04.2001 to 28.04.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
30.04.2001 to 05.05.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
30.04.2001 to 11.05.2001	Refresher Training Programme for Civil Judges (Junior Division)
11.06.2001 to 16.06.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers
11.06.2001 to 15.06.2001	Training Programme for officers of Jail and Prison
18.06.2001 to 23.06.2001	Training Programme on 'Computer Application and Information Technology' for Judicial Officers

25.06.2001 to 30.06.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers
02.07.2001 to 07.07.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers
16.07.2001 to 26.07.2001	Refresher Training Programme for Additional District and Sessions Judges
16.07.2001 to 21.07.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers
06.08.2001 to 10.08.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers
13.08.2001 to 18.08.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers
17.08.2001 to 28.08.2001	Refresher Training Programme for Civil Judges (Senior Division)
20.08.2001 to 25.08.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers

27.08.2001 to 01.09.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers
10.09.2001 to 20.09.2001	Refresher Training Programme for Civil Judges (Junior Division)
17.09.2001 to 22.09.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers.
08.10.2001 to 12.10.2001	Special Training Programme on Court and Financial Management for Additional District & Sessions Judges
08.10.2001 to 12.10.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers .
15.10.2001 to 20.10.2001	Training Programme on 'Computer and Information Technology' for Judicial officers.
16.10.2001 to 20.10.2001	Training Programme for Officers of Jail and Prison
05.11.2001 to 09.11.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers .
12.11.2001 to 17.11.2001	Special Training Programme for Additional District and Sessions Judges on Compensation Laws

19.11.2001 to 24.11.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers.
26.11.2001 to 01.12.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers.
03.12.2001 to 07.12.2001	Special Training Programme on Criminal Laws with special emphasis on Dowry Death, Rape Cases, and Offences against women for Additional District and Sessions Judges.
10.12.2001 to 15.12.2001	Training Programme on 'Computer Application and Information Technology' for Judicial officers.

Keeping in view the entry and applications of computers in courts the Institute has been organizing computer training programme for Judicial Officers of U.P. since 1999. Information Technology Act, 2000 has provided legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as electronic commerce and thus made the transactions through computers more conducive. To meet the challenges of future an international level training programme on Cyber Laws, Crimes and Intellectual Property Rights, is scheduled in the Institute from 6.01.2001 in which participants from other States of India and also from Malayasia will be participating.

Apart from imparting training a seminar on Human Rights was also organized by the institute on 02 –09-2000. Under its programme for Improving Governance in U.P.- Its legal aspects three conferences were organized by the Institute at Agra, Varanasi and Lucknow

respectively on 12-08-2000, 19-08-2000 and 23-09-2000. In the field of publication Quarterly Digest and JTRI Journal are also being published regularly by the Institute and apart from preparing other brochures the task of updating brochures and other publication of the Institute is also in hand. The research activities of the Institute are also in progress on various projects.

Many promises have to be kept, we know that sky is the limit of excellence. We are striving in the direction reminding ourselves the famous lines of Robert Frost ; "MILES TO GO BEFORE I SLEEP" .

With warm regards,

D. P. GUPTA
Director