7 years of Indian Cyber Law

Rohas Nagpal

About the author

Rohas Nagpal is the founder President of Asian School of Cyber Laws.

He advises Governments and corporates around the world in cyber crime investigation and cyber law related issues.

He has assisted the Government of India in drafting rules and regulations under the Information Technology Act, 2000.

He has authored several books, papers and articles on cyber law, cyber terrorism, cyber crime investigation and financial law.

Rohas lives in Pune (India) and blogs @ www.rohasnagpal.com

Some of the books authored by Rohas Nagpal

1. Fundamentals of Cyber Law
2. Ecommerce – Legal Issues
3. IPR & Cyberspace – Indian Perspective
4. Cyber Crime & Digital Evidence – Legal Perspective
5. Best Practices for Cyber Crime Investigation
6. Understanding Hackers and Cyber Criminals
7. Law relating to Initial Public Offering
8. Law relating to ESOP & Sweat Equity
9. Cyber Crime Manual

Some of the papers authored by Rohas Nagpal

1. Internet Time Theft & the Indian Law
2. Legislative Approach to Digital Signatures
3. Indian Legal position on Cyber Terrorism
4. Defining Cyber Terrorism
5. The mathematics of terror
6. Cyber Terrorism in the context of Globalisation
7. Biometric based Digital Signature Scheme

ABOUT THIS PAPER **2**

JURISPRUDENCE OF INDIAN CYBER LAW **3**

1. CYBER PORNOGRAPHY **6**

AVNISH BAJAJ VS. STATE (N.C.T.) OF DELHI 11

2. ACCESSING PROTECTED SYSTEM **13**

FIROS VS. STATE OF KERALA 17

3. TAMPERING WITH COMPUTER SOURCE CODE **20**

SYED ASIFUDDIN AND ORS. VS. THE STATE OF ANDHRA PRADESH & ANR. 25

4. BANKER'S BOOKS EVIDENCE ACT **29**

STATE BANK OF INDIA VS. RIZVI EXPORTS LTD 32

5. ADMISSIBILITY OF ELECTRONIC RECORDS **33**

STATE VS. MOHD. AFZAL AND OTHERS 35

6. IS ATM A COMPUTER? **40**

DIEBOLD SYSTEMS PVT LTD VS. THE COMMISSIONER OF COMMERCIAL TAXES 40

7. PLACE OF ELECTRONIC CONTRACT **42**

P.R. TRANSPORT AGENCY VS. UNION OF INDIA & OTHERS 42

About this paper

This paper is prepared for **Clubhack 2007** in December 2007.

Indian Cyber Laws were official born on 17th October 2000 with the Information Technology Act, 2000 coming into force. This paper discusses 7 interesting case laws that I feel highlight the development of cyber legal jurisprudence in India over the last 7 years.

This paper begins with a short outline of the various rules, regulations and orders that have been passed over the last 7 years. It then moves onto a brief discussion on the Indian law relating to **cyber pornography** and features the Avnish Bajaj (CEO of bazzee.com – now a part of the ebay group of companies) case.

The next issue covered by this paper is that of **protected systems** and features the Firos vs. State of Kerala case. The highly topical issue of **tampering with computer source code** is discussed next along with the Syed Asifuddin case.

The importance of the amendments to the **Banker's Books Evidence** Act is discussed next in the context of the State Bank of India vs. Rizvi Exports Ltd case.

The issue of **admissibility of electronic records** is discussed in the context of the State vs. Mohd. Afzal and others case also known as the **Parliament attack case**.

The paper ends with two cases, one focussing on **whether an ATM is a computer** and the other on the place of an **electronic contract**.

Jurisprudence of Indian Cyber Law

The primary source of cyber law in India is the **Information Technology Act**, 2000 (IT Act) which came into force on 17 October 2000.

The primary purpose of the Act is to provide **legal recognition to electronic commerce** and to facilitate filing of **electronic records with the Government**. The IT Act also penalizes various **cyber crimes** and provides strict punishments (imprisonment terms upto 10 years and compensation up to Rs 1 crore).

Minor errors in the Act were rectified by the **Information Technology (Removal of Difficulties) Order**, 2002 which was passed on 19 September 2002.

An **Executive Order** dated 12 September 2002 contained instructions relating provisions of the Act in regard to protected systems and application for the issue of a Digital Signature Certificate.

The IT Act was amended by the **Negotiable Instruments (Amendments and Miscellaneous Provisions) Act**, 2002. This introduced the concept of electronic cheques and truncated cheques.

Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004 has provided the necessary legal framework for filing of documents with the Government as well as issue of licences by the Government. It also provides for payment and receipt of fees in relation to the Government bodies.

On the same day, the **Information Technology (Certifying Authorities) Rules**, 2000 also came into force.

These rules prescribe the eligibility, appointment and working of Certifying Authorities (CA). These rules also lay down the technical standards, procedures and security methods to be used by a CA. These rules were amended in 2003, 2004 and 2006.

Information Technology (Certifying Authority) Regulations, 2001 came into force on 9 July 2001. They provide further technical standards and procedures to be used by a CA.

Two important guidelines relating to CAs were issued. The first are the **Guidelines** for submission of application for licence to operate as a Certifying Authority under the IT Act. These guidelines were issued on 9th July 2001.

Next were the **Guidelines** for submission of certificates and certification revocation lists to the Controller of Certifying Authorities for publishing in National Repository of Digital Certificates. These were issued on 16th December 2002.

The **Cyber Regulations Appellate Tribunal (Procedure) Rules**, 2000 also came into force on 17th October 2000.

These rules prescribe the appointment and working of the Cyber Regulations Appellate Tribunal (CRAT) whose primary role is to hear appeals against orders of the Adjudicating Officers.

The **Cyber Regulations Appellate Tribunal (Salary, Allowances and other terms and conditions of service of Presiding Officer) Rules**, 2003 prescribe the salary, allowances and other terms for the Presiding Officer of the CRAT.

Information Technology (Other powers of Civil Court vested in Cyber Appellate Tribunal) Rules 2003 provided some additional powers to the CRAT.

On 17th March 2003, the **Information Technology (Qualification and Experience of Adjudicating Officers and Manner of Holding Enquiry) Rules**, 2003 were passed.

These rules prescribe the qualifications and experience of Adjudicating Officers, whose chief responsibility under the IT Act is to adjudicate on cases such as unauthorized access, unauthorized copying of data, spread of viruses, denial of service attacks, disruption of computers, computer manipulation etc. These rules also prescribe the manner and mode of inquiry and adjudication by these officers.

The appointment of adjudicating officers to decide the fate of multi-crore cyber crime cases in India was the result of the **public interest litigation filed by students of Asian School of Cyber Laws** (ASCL). The Government had not appointed the Adjudicating Officers or the Cyber Regulations Appellate Tribunal for almost 2 years after the passage of the IT Act. This prompted ASCL students to file a Public Interest Litigation (PIL) in the Bombay High Court asking for a speedy appointment of Adjudicating officers.

The Bombay High Court, in its order dated 9th October 2002, directed the Central Government to announce the appointment of adjudicating officers in the public media to make people aware of the appointments. The division bench of the Mumbai High Court consisting of Hon'ble Justice

A.P. Shah and Hon'ble Justice Ranjana Desai also ordered that the Cyber Regulations Appellate Tribunal be constituted within a reasonable time frame.

Following this the Central Government passed an order dated 23rd March 2003 appointing the "Secretary of Department of Information Technology of each of the States or of Union Territories" of India as the adjudicating officers.

The **Information Technology (Security Procedure) Rules**, 2004 came into force on 29th October 2004. They prescribe provisions relating to secure digital signatures and secure electronic records.

> Also relevant are the **Information Technology (Other Standards) Rules**, 2003.

An important **order relating to blocking of websites** was passed on 27th February, 2003.

> Computer Emergency Response Team (CERT-IND) can instruct Department of Telecommunications (DOT) to block a website.

The **Indian Penal Code** (as amended by the IT Act) penalizes several cyber crimes. These include forgery of electronic records, cyber frauds, destroying electronic evidence etc.

Digital Evidence is to be collected and proven in court as per the provisions of the **Indian Evidence Act** (as amended by the IT Act).

In case of bank records, the provisions of the **Bankers' Book Evidence Act** (as amended by the IT Act) are relevant.

Investigation and adjudication of cyber crimes is done in accordance with the provisions of the **Code of Criminal Procedure** and the IT Act.

The Reserve Bank of India Act was also amended by the IT Act.

1. Cyber Pornography

There is no settled definition of pornography or obscenity. What is considered simply sexually explicit but not obscene in USA may well be considered obscene in India. There have been many attempts to limit the availability of pornographic content on the Internet by governments and law enforcement bodies all around the world but with little effect.

Pornography on the Internet is available in different formats. These range from pictures and short animated movies, to sound files and stories. The Internet also makes it possible to discuss sex, see live sex acts, and arrange sexual activities from computer screens. Although the Indian Constitution guarantees the fundamental right of freedom of speech and expression, it has been held that a law against obscenity is constitutional. The Supreme Court has defined obscene as “offensive to modesty or decency; lewd, filthy, repulsive.

Section 67 of the IT Act is the most serious Indian law penalizing cyber pornography. Other Indian laws that deal with pornography include the **Indecent Representation of Women (Prohibition) Act** and the **Indian Penal Code.**

> According to Section 67 of the IT Act
>
> *Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.*

This section explains what is considered to be obscene and also lists the acts in relation to such obscenity that are illegal.

What constitutes obscenity in electronic form?

To understand what constitutes obscenity in the electronic form, let us analyse the relevant terms:

> **Any material** in the context of this section would include video files, audio files, text files, images, animations etc. These may be stored on CDs, websites, computers, cell phones etc.

Lascivious is something that tends to excite lust.

Appeals to, in this context, means “arouses interest”.

Prurient interest is characterized by lustful thoughts.

Effect means to produce or cause.

Tend to deprave and corrupt in the context of this section means “to lead someone to become morally bad”.

Persons here refers to natural persons (men, women, children) and not artificial persons (such as companies, societies etc).

Having understood these terms, let us analyse what constitutes obscenity. To be considered obscene for the purpose of this section, the matter must satisfy at least one of the following conditions:

1. it must tend to excite lust, or
2. it must arouse interest in lustful thoughts, or
3. it must cause a person to become morally bad.

The above conditions must be satisfied in respect of a person who is the likely target of the material. This can be understood from the following illustration:

Illustration
Sameer launches a website that contains information on sex education. The website is targeted at higher secondary school students. Pooja is one such student who is browsing the said website. Her illiterate young maid servant happens to see some explicit photographs on the website and is filled with lustful thoughts.

This website would not be considered obscene. This is because it is most likely to be seen by educated youngsters who appreciate the knowledge sought to be imparted through the photographs. It is under very rare circumstances that an illiterate person would see these explicit images.

Acts that are punishable in respect of obscenity

To understand the acts that are punishable in respect of obscenity in the electronic form, let us analyse the relevant terms:

Publishes means “to make known to others”. It is essential that at least one natural person (man, woman or child) becomes aware or understands the information that is published. Simply putting up a website that is never visited by any person does not amount to publishing.

Illustration

Sameer has just hosted a website containing his articles written in English. Sameer has not published the articles.

An automated software released by an Internet search engine indexes Sameer’s website. Sameer has still not published the articles.

A Chinese man, who does not understand a word of English, accidentally visits Sameer’s website. Sameer has still not published the articles.

Pooja, who understands English, visits Sameer’s website and reads some of his articles. Now, Sameer has published his articles.

Transmits means to pass along, convey or spread. It is not necessary that the “transmitter” actually understands the information being transmitted.

Illustration

Sameer has just hosted a website containing his articles. Pooja uses an Internet connection provided by Noodle Ltd to visit Sameer’s website. Noodle Ltd has transmitted Sameer’s articles to Pooja. However, Noodle employees are not actually aware of the information being transmitted by their computers.

Causes to be published means “to bring about the publishing of something”. It is essential that the actual publishing must take place.

Illustration

Sameer has just hosted a website containing his articles. An automated software released by Noodle Internet search engine indexes Sameer’s website. But no human being has still used that index to read these articles. Noodle has not caused Sameer’s articles to be published.

Based upon the index created by Noodle, Pooja reaches Sameer's website and reads some of his articles. Now, Noodle has caused Sameer's articles to be published.

Information **in the electronic form** includes websites, songs on a CD, movies on a DVD, jokes on a cell phone, photo sent as an email attachment etc.

The **punishment** provided under this section is as under:

1. First offence: Simple or rigorous imprisonment up to **5 years** and fine up to **Rs 1 lakh**

2. Subsequent offence: Simple or rigorous imprisonment up to **10 years** and fine up to **Rs 2 lakh**

Publishing cyber pornography (Summary)

Actions covered	Publishing, causing to be published and transmitting cyber pornography.
Penalty	First offence: Simple or rigorous imprisonment up to **5 years** and fine up to **Rs 1 lakh** Subsequent offence: Simple or rigorous imprisonment up to **10 years** and fine up to **Rs 2 lakh**
Relevant authority	Court of Session
Appeal lies to	High Court
Investigation Authorities	1. Controller of Certifying Authorities (CCA) 2. Person authorised by CCA 3. Police Officer not below the rank of Deputy Superintendent
Points to mention in complaint	1. Complainant details 2. Suspect details 3. How and when the contravention was discovered and by whom 4. Other relevant information

Avnish Bajaj vs. State (N.C.T.) of Delhi
(2005)3CompLJ364(Del), 116(2005)DLT427, 2005(79)DRJ576

IN THE HIGH COURT OF DELHI
Bail Appl. No. 2284 of 2004
Decided On: 21.12.2004
Appellants: **Avnish Bajaj**
Vs.
Respondent: **State (N.C.T.) of Delhi**

Summary of the case

Avnish Bajaj, CEO of Baazee.com, an online auction website, was arrested for distributing cyber pornography. The charges stemmed from the fact that someone had sold copies of a pornographic CD through the Baazee.com website.

The court granted him bail in the case.

The major factors considered by the court were:

1. There was no prima facie evidence that Mr. Bajaj directly or indirectly published the pornography,

2. The actual obscene recording/clip could not be viewed on Baazee.com,

3. Mr. Bajaj was of Indian origin and had family ties in India.

Background

Avnish Bajaj is the CEO of Baazee.com, a customer-to-customer website, which facilitates the online sale of property. Baazee.com receives commission from such sales and also generates revenue from advertisements carried on its web pages.

An obscene MMS clipping was listed for sale on Baazee.com on 27th November, 2004 in the name of “DPS Girl having fun". Some copies of the clipping were sold through Baazee.com and the seller received the money for the sale.

Avnish Bajaj was arrested under section 67 of the Information Technology Act, 2000 and his bail application was rejected by the trial court. He then approached the Delhi High Court for bail.

Issues raised by the Prosecution

1. The accused did not stop payment through banking channels after learning of the illegal nature of the transaction.

2. The item description "DPS Girl having fun" should have raised an alarm.

Issues raised by the Defence

1. Section 67 of the Information Technology Act relates to publication of obscene material. It does not relate to transmission of such material.

2. On coming to learn of the illegal character of the sale, remedial steps were taken within 38 hours, since the intervening period was a weekend.

Findings of the court

1. It has not been established from the evidence that any publication took place by the accused, directly or indirectly.

2. The actual obscene recording/clip could not be viewed on the portal of Baazee.com.

3. The sale consideration was not routed through the accused.

4. Prima facie Baazee.com had endeavored to plug the loophole.
5. The accused had actively participated in the investigations.

6. The nature of the alleged offence is such that the evidence has already crystallized and may even be tamper proof.

7. Even though the accused is a foreign citizen, he is of Indian origin with family roots in India.

8. The evidence that has been collected indicates only that the obscene material may have been unwittingly offered for sale on the website.

9. The evidence that has been collected indicates that the heinous nature of the alleged crime may be attributable to some other person.

Decision of the court

1. The court granted bail to Mr. Bajaj subject to furnishing two sureties of Rs. 1 lakh each.

2. The court ordered Mr. Bajaj to surrender his passport and not to leave India without the permission of the Court.

3. The court also ordered Mr. Bajaj to participate and assist in the investigation.

2. Accessing Protected System

According to section 70 of the IT Act

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.

(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-Section (1).

(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this Section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

As per Executive order dated 12-9-2002, issued by Ministry of Communications &Information Technology details of every protected system should be provided to the Controller of Certifying Authorities.

There are three elements to this section-

1. Gazette notification for declaring protected system.
2. Government order authorizing persons to access protected systems.
3. Punishment for access to protected systems by unauthorised persons.

Let us discuss the relevant terms and issues in detail.

Appropriate government is determined as per Schedule VII of the Constitution of India.

Schedule VII of the Constitution of India contains 3 lists – Union, State and Concurrent. Parliament has the exclusive right to make laws on items covered in the Union List e.g. defence, Reserve Bank of India etc.

State Governments have the exclusive right to make laws on items covered in the State List e.g. police, prisons etc.

Parliament as well as the State Governments can make laws on matters in the Concurrent List e.g. forests, electricity etc.

Illustration 1
If the computer network of the Indian Army is to be declared as a protected system, the Central Government would be the appropriate Government.

Illustration 2
If the computer network of the Mumbai police is to be declared as a protected system, the Government of Maharashtra would be the appropriate Government.

Illustration 3
If the computer network of the Forest Department in Maharashtra is to be declared as a protected system, the Central Government as well as the Government of Maharashtra would be the appropriate Government.

All the acts, rules, regulations etc passed by the Central and State Government are notified in the **Official Gazette.** The Official Gazette in the electronic form is called the Electronic Gazette. A notification becomes effective on the date of its publication in the Gazette.

The Government **order** may specify the authorised persons by name or by designation (e.g. all officers of rank of Inspector and above deputed in a particular department).

The term "**securing access**" in this section is a grammatical variation of the term "secures access" as discussed earlier.

Attempt to secure access is a very wide term and can best be understood through the following illustrations.

Illustration 1
Sameer runs a password cracking software to crack the password of a protected system. Irrespective of whether he succeeds in cracking the password, he is guilty of attempting to secure access.

Illustration 2
Sameer runs automated denial of service software to bring down the firewall and securing a protected system. Irrespective of whether he succeeds in bringing down the firewall, he is guilty of attempting to secure access.

Illustration 3
Sameer sends a Trojan by email to Pooja, who is the network administrator of a protected system. He plans to Trojanize Pooja's computer and thereby gain unauthorised access to the protected system. Irrespective of whether he succeeds in finally accessing the protected system, he is guilty of attempting to secure access.

The **punishment** provided for this section is rigorous or simple imprisonment of up to **10 years** and **fine**.

Unauthorised Access to Protected System (Summary)

Actions covered	Unauthorised access to protected system (or attempt thereof)
Penalty	Imprisonment up to **10 years** and **fine** (this may be rigorous or simple imprisonment i.e. with or without hard labour)
Relevant authority	Court of Session
Appeal lies to	High Court
Investigation Authorities	1. Controller of Certifying Authorities (CCA) 2. Person authorised by CCA 3. Police Officer not below the rank of Deputy Superintendent
Points to mention in complaint	1. Complainant details 2. Suspect details 3. Details of gazette notification and Government order 4. How and when the contravention was discovered and by whom 5. Other relevant information

Firos vs. State of Kerala
AIR2006Ker279, 2006(3)KLT210, 2007(34)PTC98(Ker)

IN THE HIGH COURT OF KERALA

W.A. No. 685 of 2004
Decided On: 24.05.2006

Appellants: **Firos**
Vs.
Respondent: **State of Kerala**

Summary of the case

The Government of Kerala issued a notification u/s 70 of the Information Technology Act declaring the FRIENDS application software as a protected system.

The author of the application software filed a petition in the High Court against the said notification. He also challenged the constitutional validity of section 70 of the IT Act.

The Court upheld the validity of both, section 70 of the IT Act, as well as the notification issued by the Kerala Government.

Background of the case

Government of Kerala, as part of IT implementation in Government departments, conceived a project idea of "FRIENDS" (Fast, Reliable, Instant, Efficient Network for Disbursement of Services).

The project envisaged development of a software for single window collection of bills payable to Government, local authorities, various statutory agencies, Government Corporations etc. towards tax, fees, charges for electricity, water, etc. A person by making a consolidated payment in a computer counter served through "FRIENDS" system can discharge all his liabilities due to the Government, local authorities and various agencies.

The work of developing the "FRIENDS" software was entrusted to Firos. The application-software "FRIENDS" was first established at Thiruvananthapuram, free of cost, and since the project was successful, the Government decided to set up the same in all other 13 district centres.

The Government of Kerala entered into a contract with Firos for setting up and commissioning "FRIENDS" software system in 13 centres all over Kerala for providing integrated services to the customers through a single window for a total consideration of Rs. 13 lakh. Firos set up FRIENDS service centres in all the 13 centres and they were paid the agreed remuneration.

A dispute arose between Firos and the Government with regard to Intellectual Property Rights (IPR) in the FRIENDS software.

The Government arranged to modify the FRIENDS software to suit its further requirements through another agency. Firos alleged violation of copyright and filed a criminal complaint against the Government. A counter case was filed by the Government against Firos.

The Government of Kerala issued a notification under Section 70 of the Information Technology Act declaring the FRIENDS software installed in the computer system and computer network established in all centres in Kerala as a protected system.

Firos filed a writ petition challenging section 70 of the IT Act.

Issues raised by the Petitioner

1. The Government of Kerala notification under section 70 of the IT Act is arbitrary, discriminatory and violates Article 19(1)(g) of the Constitution of India.

2. The Government of Kerala notification under section 70 of the IT Act is and was against the statutory right conferred under Section 17 of the Copyright Act.

3. Section 70 of the IT Act which confers the unfettered powers on the State Government to declare any computer system as a protected system is arbitrary and unconstitutional and inconsistent with Copyright Act.

4. Section 70 of the IT Act has to be declared as illegal.

5. There is direct conflict between the provisions of Section 17 of the Copyright Act and Section 70 of the Information Technology Act. When there is conflict between two Acts, a harmonious construction has to be adopted.

Conclusions of the court

1. There is no conflict between the provisions of Copyright Act and Section 70 of IT Act.

2. Section 70 of the IT Act is not unconstitutional.

3. While interpreting section 70 of the IT Act, a harmonious construction with Copyright Act is needed.

4. Section 70 of the IT Act is not against but subject to the provisions of the Copyright Act.

5. Government cannot unilaterally declare any system as "protected" other than "Government work" falling under section 2(k) of the Copyright Act on which Govt.'s copyright is recognised under Section 17(d) of the said Act.

Section 2(k) of the Copyright Act

(k) 'Government work' means a work which is made or published by or under the direction or control of -

(i) the Government or any department of the Government;

(ii) any Legislature in India;

(iii) any Court, Tribunal or other judicial authority in India;

Section 17(d) of the Copyright Act

17. First owner of copyright:- Subject to the provisions of this Act, the author of a work shall be the owner of the copyright therein;

(d) in the case of a Government work, Government shall, in the absence of any agreement to the contrary, be the first owner of the copyright therein;

3. Tampering with computer source code

According to section 65 of the IT Act

Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation.—For the purposes of this section, "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Computer source code is the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Computer source code need not only be in the electronic form. It can be printed on paper (e.g. printouts of flowcharts for designing a software application).

Let us understand this using some illustrations:

Illustration 1

Pooja has created a simple computer program. When a user double-clicks on the hello.exe file created by Pooja, the following small screen opens up:

Hello World

The hello.exe file created by Pooja is the executable file that she can give to others. The small screen that opens up is the output of the software program written by Pooja.

Pooja has created the executable file using the programming language called “C”. Using this programming language, she created the following lines of code:

```
main()
{
        printf("hello, ");
        printf("world");
        printf("\n");
}
```

These lines of code are referred to as the source code.

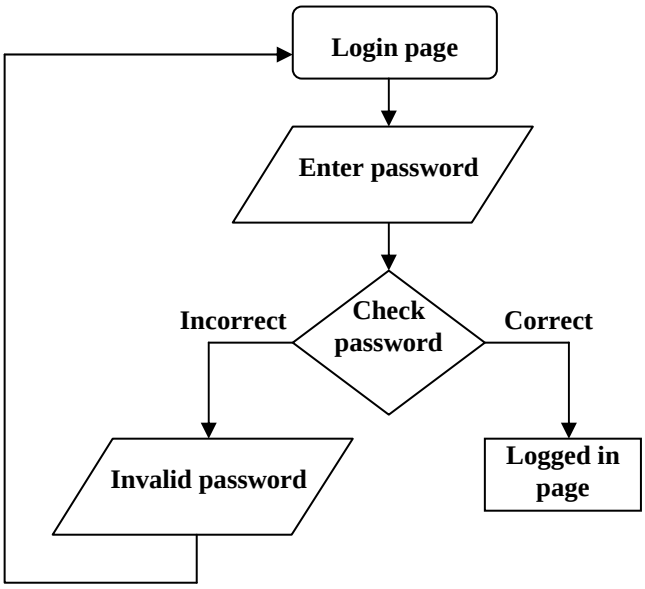
Illustration 2

Noodle Ltd has created software for viewing and creating image files. The programmers who developed this program used the computer-programming language called Visual C++. Using the syntax of these languages, they wrote thousands of lines of code.

This code is then compiled into an executable file and given to end-users. All that the end user has to do is double-click on a file (called setup.exe) and the program gets installed on his computer. The lines of code are known as computer source code.

Illustration 3

Pooja is creating a simple website. A registered user of the website would have to enter the correct password to access the content of the website. She creates the following flowchart outlining the functioning of the authentication process of the website.



She takes a printout of the flowchart to discuss it with her client. The printout is source code.

This section relates to computer source code that is either:

1. required to be kept (e.g. in a cell phone, hard disk, server etc), **or**
2. required to be maintained by law

The following acts are prohibited in respect of the source code

1. knowingly concealing or destroying or altering
2. intentionally concealing or destroying or altering
3. knowingly causing another to conceal or destroy or alter
4. intentionally causing another to conceal or destroy or alter

Let us discuss the relevant terms and issues in detail.

Conceal simply means "to hide"

Illustration
Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer changes the properties of the folder and makes it a "hidden" folder.

Although the source code folder still exists on Pooja's computer, she can no longer see it. Sameer has concealed the source code.

Destroys means "to make useless", "cause to cease to exist", "nullify", "to demolish", or "reduce to nothing".

Destroying source code also includes acts that render the source code useless for the purpose for which it had been created.

Illustration 1
Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes the folder. He has destroyed the source code.

Illustration 2
Pooja has created a software program. The source code files of the program are contained in a folder on Pooja's laptop. Sameer deletes one of the source code

files. Now the source code cannot be compiled into the final product. He has destroyed the source code.

Illustration 3
Pooja is designing a software program. She draws out the flowchart depicting the outline of the functioning of the program. Sameer tears up the paper on which she had drawn the flowchart. Sameer has destroyed the source code.

Alters, in relation to source code, means “modifies”, “changes”, “makes different” etc. This modification or change could be in respect to size, properties, format, value, utility etc”.

Illustration
Pooja has created a webpage for her client. The source code of the webpage is in HTML (Hyper Text Markup Language) format. Sameer changes the file from HTML to text format. He has altered the source code.

Tampering with computer source code (Summary)

Actions covered	Knowingly or intentionally concealing, altering or destroying computer source code (or causing someone else to do so).
Penalty	Imprisonment up to **3 years** and / or fine up to **Rs 2 lakh**
Relevant authority	Judicial Magistrate First Class
Appeal lies to	Court of Session
Investigation Authorities	1. Controller of Certifying Authorities (CCA) 2. Person authorised by CCA 3. Police Officer not below the rank of Deputy Superintendent
Points to mention in complaint	1. Complainant details 2. Suspect details 3. How and when the contravention was discovered and by whom 4. Damage suffered 5. Other relevant information

Syed Asifuddin and Ors. Vs. The State of Andhra Pradesh & Anr.
2005CriLJ4314

IN THE HIGH COURT OF ANDHRA PRADESH
Cri. Petn. Nos. 2601 and 2602 of 2003
Decided On: 29.07.2005

Appellants: **Syed Asifuddin and Ors.**
Vs.
Respondent: **The State of Andhra Pradesh and Anr.**

Summary of the case

Tata Indicom employees were arrested for manipulation of the electronic 32-bit number (ESN) programmed into cell phones that were exclusively franchised to Reliance Infocomm.

The court held that such manipulation amounted to tampering with computer source code as envisaged by section 65 of the Information Technology Act, 2000.

Background of the case

Reliance Infocomm launched a scheme under which a cell phone subscriber was given a digital handset worth Rs. 10,500 as well as service bundle for 3 years with an initial payment of Rs. 3350 and monthly outflow of Rs. 600. The subscriber was also provided a 1 year warranty and 3 year insurance on the handset.

The condition was that the handset was technologically locked so that it would only work with the Reliance Infocomm services. If the customer wanted to leave Reliance services, he would have to pay some charges including the true price of the handset. Since the handset was of a high quality, the market response to the scheme was phenomenal.

Unidentified persons contacted Reliance customers with an offer to change to a lower priced Tata Indicom scheme. As part of the deal, their phone would be technologically “unlocked” so that the exclusive Reliance handsets could be used for the Tata Indicom service.

Reliance officials came to know about this “unlocking” by Tata employees and lodged a First Information Report (FIR) under various provisions of the Indian Penal Code, Information Technology Act and the Copyright Act.

The police then raided some offices of Tata Indicom in Andhra Pradesh and arrested a few Tata Tele Services Limited officials for re-programming the Reliance handsets.

These arrested persons approached the High Court requesting the court to quash the FIR on the grounds that their acts did not violate the said legal provisions.

Issues raised by the Defence

1. It is always open for the subscriber to change from one service provider to the other service provider.

2. The subscriber who wants to change from Tata Indicom always takes his handset, to other service providers to get service connected and to give up Tata services.

3. The handsets brought to Tata by Reliance subscribers are capable of accommodating two separate lines and can be activated on principal assignment mobile (NAM 1 or NAM 2). The mere activation of NAM 1 or NAM 2 by Tata in relation to a handset brought to it by a Reliance subscriber does not amount to any crime.

4. A telephone handset is neither a computer nor a computer system containing a computer programme.

5. There is no law in force which requires the maintenance of "computer source code". Hence section 65 of the Information Technology Act does not apply.

Findings of the court

1. As per section 2 of the Information Technology Act, any electronic, magnetic or optical device used for storage of information received through satellite, microwave or other communication media and the devices which are programmable and capable of retrieving any information by manipulations of electronic, magnetic or optical impulses is a computer which can be used as computer system in a computer network.

2. The instructions or programme given to computer in a language known to the computer are not seen by the users of the computer/consumers of computer functions. This is known as source code in computer parlance.

3. A city can be divided into several cells. A person using a phone in one cell will be plugged to the central transmitter of the telecom provider. This central transmitter will receive the signals and then divert them to the relevant phones.

4. When the person moves from one cell to another cell in the same city, the system i.e., Mobile Telephone Switching Office (MTSO) automatically transfers signals from tower to tower.

5. All cell phone service providers have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider.

6. System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Every cell phone operator is required to obtain SID from the Government of India. SID is programmed into a phone when one purchases a service plan and has the phone activated.

7. Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. ESN is a permanent part of the phone.

8. Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. MIN is programmed into a phone when one purchases a service plan.

9. When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing.

10. If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range.

11. When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring.

12. So as to match with the system of the cell phone provider, every cell phone contains a circuit board, which is the brain of the phone. It is a combination of several computer chips programmed to convert analog to digital and digital to analog conversion and translation of the outgoing audio signals and incoming signals.

13. This is a micro processor similar to the one generally used in the compact disk of a desktop computer. Without the circuit board, cell phone instrument cannot function.

14. When a Reliance customer opts for its services, the MIN and SID are programmed into the handset. If some one manipulates and alters ESN, handsets which are exclusively used by them become usable by other service providers like TATA Indicom.

Conclusions of the court

1. A cell phone is a computer as envisaged under the Information Technology Act.

2. ESN and SID come within the definition of “computer source code” under section 65 of the Information Technology Act.

3. When ESN is altered, the offence under Section 65 of Information Technology Act is attracted because every service provider has to maintain its own SID code and also give a customer specific number to each instrument used to avail the services provided.

4. Whether a cell phone operator is maintaining computer source code, is a matter of evidence.

5. In Section 65 of Information Technology Act the disjunctive word "or" is used in between the two phrases –

    a. "when the computer source code is required to be kept"

    b. "maintained by law for the time being in force"

4. Banker's Books Evidence Act

The Banker's Books Evidence Act lays down the rules of evidence in relation to **bankers' books**. Generally, bankers' books would be adduced as evidence where any financial transaction involving the banking system is in question or has to be examined.

The IT Act has amended the Banker's Book Evidence Act to confer equal status on electronic records as compared to paper based documents.

Bankers' books include ledgers, day-books, cash-books, account-books and all other books used in the ordinary business of a bank. These can be in paper form or printouts of data stored in bank computers.

If a "certified copy" of printouts of bankers' books has to be given, then such printouts must be accompanied by **three certificates.**

Let us take a simple illustration to understand the contents of these certificates.

Note: These certificates are for illustration purposes only and do not constitute legal advise. Please **do not** use in a real scenario. If you require legally valid certificate formats for use in a real scenario, please email us on info@asianlaws.org

Illustration

Sameer issued a cheque to Pooja for Rs 3 lakh. The cheque was dishonoured by Sameer's bank (Noodle Bank Ltd) as the balance in Sameer's account was only Rs 50,000. Pooja has filed a case against Sameer under section 138 of the Negotiable Instruments Act for the cheque "bouncing".

Pooja has requested Noodle Bank for a certified copy of Sameer's bank account statement (for January 2008) for producing in court as evidence. The printout of the bank statement will be accompanied by the following 3 certificates:

Certificate u/s 2A(a) of the Banker's Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that:

1. Mr. Sameer Sen is holding account no. 12345 with the Pune branch of the Noodle Bank Ltd.

2. The accompanying bank account statement is a printout of the transactions and balances in the said bank account for the period beginning 1st January 2008 and ending 31st January 2008.

Siddharth Sharma
Manager, Pune branch
Noodle Bank Ltd

Certificate u/s 2A(b) of the Banker's Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that the enclosed "Information Security Policy of Noodle Bank Ltd" contains the true and correct information relating to the computer system used to store bank account related information of Noodle Bank customers and including the following information:

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed only by authorised persons;

(B) the safeguards adopted to prevent and detect unauthorised change of data;

(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;

(D) the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electro-magnetic data storage devices;

(E) the mode of verification in order to ensure that data has been accurately transferred to such removable media;

(F) the mode of identification of such data storage devices;

(G) the arrangements for the storage and custody of such storage devices;

(H) the safeguards to prevent and detect any tampering with the system; and

(l) other factors that will vouch for the integrity and accuracy of the system.

Pooja Singh
System Administrator, Pune branch
Noodle Ltd

Enclosed: Information Security Policy of Noodle Bank Ltd

Certificate u/s 2A(c) of the Banker's Books Evidence Act

I, the undersigned, state to the best of my knowledge and belief that:

1. The Noodle computer system described more accurately in the "Information Security Policy of Noodle Bank Ltd" operated properly at the material time when the said system was used to take the printout relating to the transactions and balances in the bank account no. 12345 for the period beginning 1st January 2008 and ending 31st January 2008 was taken.

2. The printout referred to above is appropriately derived from the relevant data stored in the said system.

Pooja Singh
System Administrator, Pune branch
Noodle Ltd

State Bank of India vs. Rizvi Exports Ltd
II(2003)BC96

DEBT RECOVERY APPELLATE TRIBUNAL, ALLAHABAD

T.A. No. 1593 of 2000
Decided On: 01.10.2002

Appellants: State Bank of India
Vs.
Respondent: Rizvi Exports Ltd.

State Bank of India (SBI) had filed a case to recover money from some persons who had taken various loans from it. As part of the evidence, SBI submitted printouts of statement of accounts maintained in SBI's computer systems.

The relevant certificates as mandated by the Bankers Books of Evidence Act (as amended by Information Technology Act) had not been attached to these printouts.

The Court held that these documents were not admissible as evidence.

5. Admissibility of electronic records

Section 65B of the Indian Evidence Act relates to admissibility of electronic records as evidence in a Court of law.

The computer holding the original evidence does not need to be produced in court. A printout of the record, or a copy on a CD ROM, hard disk, floppy etc can be produced in court. However some conditions need to be met and a certificate needs to be provided. These conditions and the certificate are best explained using a detailed illustration.

Note: This certificate is for illustration purposes only and does not constitute legal advice. Please **do not** use in a real scenario. If you require a legally valid certificate format for use in a real scenario, please email us on info@asianlaws.org

Illustration

Noodle Ltd is an Internet Service Provider. The police are investigating a cyber crime and need details about the user of a particular IP address. They have requested Noodle for these details.

What Noodle is going to provide the police is a printout of records stored in its computer systems. The following authenticated certificate has to be attached to this printout.

Certificate u/s 65B of Indian Evidence Act issued in relation to the printout titled "Information relating to IP address 10.232.211.84"

I, the undersigned, state to the best of my knowledge and belief that:

1. The printout titled "Information relating to IP address 10.232.211.84" issued on 1st January 2008 contains information stored in the ABC server being used by Noodle Ltd to provide Internet connection services to its customers in India.

2. The said printout was produced by the ABC server during the period over which the ABC server was used regularly to store and process information for the purposes of activities regularly carried on over that period by lawfully authorised persons.

3. During the said period, information of the kind contained in the electronic record was regularly fed into the ABC server in the ordinary course of the said activities.

4. Throughout the material part of the said period, the computer was operating properly.

5. The information contained in the electronic record reproduces such information fed into the computer in the ordinary course of the said activities.

6. I am in a responsible official position in relation to the operation of the ABC server.

   Signed on this 1st day of January 2008

   Pooja Singh
   System Administrator,
   Noodle Ltd

State vs. Mohd. Afzal and others
2003VIIAD(Delhi)1, 107(2003)DLT385, 2003(71)DRJ178, 2003(3)JCC1669

IN THE HIGH COURT OF DELHI
Reference No. 1/2003 and Crl. A. No. 43/2003
Decided On: 29.10.2003
Appellants: State
Vs.
Respondent: Mohd. Afzal and Ors.
[Alongwith Crl. A. Nos. 59 and 80/2003]
AND
Appellants: Mohd. Afzal
Vs.
Respondent: State
[Along with Crl. A. Nos. 12, 19 and 36/2003]

Summary of the case

Several terrorists had attacked the Parliament House on 13th December, 2001. Digital evidence played an important role during their prosecution. The accused had argued that computers and digital evidence can easily be tampered and hence should not be relied upon.

The Court dismissed these arguments. It said that challenges to the accuracy of computer evidence on the ground of misuse of system or operating failure or interpolation, should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

Background of the case

Several terrorists had attacked the Parliament House on 13th December, 2001 intending to take as hostage or kill the Prime Minister, Central Ministers, Vice-President of India and Members of Parliament. Several terrorists were killed by the police in the encounter and several persons were arrested in connection with the attack.

The Designated Judge of the Special Court constituted under Section 23 of the Prevention of Terrorist Activities Act, 2002 (POTA) had convicted several accused persons. They filed an appeal in the Delhi High Court challenging the legality and validity of the trial and the sustainability of the judgment.

Digital evidence played an important role in this case. Computerized cell phone call logs were heavily relied upon in this case.

A laptop, several smart media storage disks and devices were recovered from a truck intercepted at Srinagar pursuant to information given by two of the suspects. These articles were deposited in the police “malkhana” on 16th December, 2001. Although the laptop was deposited in the “malkhana” on 16th December, some files were written onto the laptop on 21st December.

The laptops were forensically examined by a private computer engineer and the Assistant Government Examiner of Questioned Documents, Bureau of Police Research, Hyderabad.

The laptop contained files relating to identity cards and stickers that were used by the terrorists to enter the Parliament premises. Cyber forensic examination showed that the laptop was used for creating, editing and viewing image files (mostly identity cards).

Evidence found on the laptop included:

1. fake identity cards,
2. video files containing clippings of political leaders with Parliament in background shot from TV news channels,
3. scanned images of front and rear of a genuine identity card,
4. image file of design of Ministry of Home Affairs car sticker,
5. the game 'wolf pack' with the user name 'Ashiq'. Ashiq was the name in one of the fake identity cards used by the terrorists.

Issues raised by the Prosecution

2. Analysis of the Windows registry files of the suspect laptop showed that its hard disk had not been changed.

3. If internet has been accessed through a computer then the actual date of such access would be reflected. Additionally, if any change is made to the date setting of the computer, it would be reflected in the history i.e. in the REG file.

4. A hard disc cannot be changed without it being reflected in the history maintained in the REG file.

5. It was not possible to alter the date of any particular file unless the system date had been altered.

6. The files written on the laptop on 21st December were “self generating and self written” system files. These were created automatically by the laptop’s operating system when the laptop was accessed by law enforcement agencies at the “malkhana”.

Issues raised by the Defence

2. Although the laptop was deposited in the Government “malkhana” on 16th December, some files were written on the laptop on 21st December.

3. The date setting on a computer can be edited.

4. In the absence of verified time setting and reliable information about the hard disc being original, there is no certainty that the material found on a later date, was exactly the material, which may have existed on a previous date.

5. Hard disc is a replaceable component and could be formatted. If a hard disc was replaced, it would not contain the data which was stored earlier unless it was re-fed.

6. The Windows registry files can be edited.

7. The back up of complete suspect hard disc was not taken by the law enforcement agencies.

8. The date setting on a file is related to the date setting on the computer. It is possible to modify this date.

9. Information stored in a computer is on a magnetic medium which can easily be polarized. Therefore, any data in a computer can be changed by a knowledgeable person.

10. The date of last access to a file is treated differently by different software. The time of last access was meaningless in the absence of knowledge as to what software is used to process the file.

11. Software which was installed in a computer could be modified and un-installed without leaving any trace.

Points considered by the court

1. In effect, substantially, Section 65B of the Indian Evidence Act and Section 69 of the Act in England have same effect.

2. Section 69 of The Police & Criminal Evidence Act, 1984 of England 280 reads as under:

   In any proceedings, a statement in a document produced by a computer shall not be admissible as evidence of any fact stated therein unless it is shown

   (a) that there are no reasonable grounds for believing that the statement is inaccurate because of improper use of the computer.

(b) that at all material times the computer was operating properly, or if not, that any respect in which it was not operating properly or was out of operation was not such as to affect the production of the document or the accuracy of it contents;....

3. It was held by Lord Griffiths In R.V. Shepherd, 1993 A.C. 380., that computers vary immensely in their complexity and in the operations they perform. The nature of the evidence to discharge the burden of showing that there has been no improper use of the computer and that it was operating properly will inevitably vary from case to case. He further stated that “I suspect that it will very rarely be necessary to call an expert and that in the vast majority of cases it will be possible to discharge the burden by calling a witness who is familiar with the operation of the computer in the sense of knowing what the computer is required to do and who can say that it is doing it properly."

4. In DPP v. Me. Kewon, (1997) 1 Criminal Appeal 155, Lord Hoffman discussed this section 69. He said that it cannot be argued that “any malfunction is sufficient to cast doubt upon the capacity of the computer to process information correctly. A malfunction is relevant if it affects the way in which the computer processes, stores or retrieves the information used to generate the statement tendered in evidence. Other malfunctions do not matter”.

5. The Law Commission in England held that “Realistically, therefore, computers must be regarded as imperfect devices." The Law Commission recommended the deletion of this section 69 and subsequently it was deleted.

6. The Law Commission report in England said that “The complexity of modern systems makes it relatively easy to establish a reasonable doubt in a juror's mind as to whether the computer was operating properly.... We are concerned about smoke-screens being raised by cross-examination which focuses in general terms on the fallibility of computers rather than the reliability of the particular evidence. The absence of a presumption that the computer is working means that it is relatively easy to raise a smoke-screen."

7. In England, the common law presumption that "in the absence of evidence to the contrary the courts will

presume that mechanical instruments were in order at the material time", operates with full force.

8. Development in computer networking, access, control, monitoring and systems security are increasingly making it difficult for computer errors to go undetected. Most computer errors are immediately detected or the resultant error in the date is immediately recorded.

Conclusion of the court

If someone challenges the accuracy of computer evidence on the ground of misuse of system or operating failure or interpolation, then the challenger has to establish the challenge.

Mere theoretical and generic doubts cannot be cast on the evidence.

6. Is ATM a computer?

Diebold Systems Pvt Ltd vs. The Commissioner of Commercial Taxes

ILR2005KAR2210, [2006]144STC59(Kar)

IN THE HIGH COURT OF KARNATAKA

Sales Tax Appeal No. 2/2004

Decided On: 31.01.2005

Appellants: **Diebold Systems Pvt. Ltd.**

Vs.

Respondent: **The Commissioner of Commercial Taxes**

Section 2 of Information Technology Act, 2000

Background

Diebold Systems Pvt Ltd manufactures and supplies Automated Teller Machines (ATM).

Diebold sought a clarification from the Advance Ruling Authority (ARA) in Karnataka on the rate of tax applicable under the Karnataka Sales Tax Act, 1957 on sale of Automated Teller Machines.

The majority view of the ARA was to classify ATMs as "computer terminals" liable for 4% basic tax as they would fall under Entry 20(ii)(b) of Part 'C' of Second Schedule to the Karnataka Sales Tax Act.

The Chairman of the ARA dissented from the majority view. In his opinion, ATMs would fit into the description of electronic goods, parts and accessories thereof. They would thus attract basic rate of tax of 12% and would fall under Entry 4 of Part 'E' of the Second Schedule to the KST Act.

The Commissioner of Commercial Taxes was of the view that the ARA ruling was erroneous and passed an order that ATMs cannot be classified as computer terminals.

Findings of the court

1. The enlarged definition of "computers" in the Information Technology Act cannot be made use of interpreting an Entry under fiscal legislation.

2. An Automatic Teller Machine is an electronic device, which allows a bank's customer to make cash withdrawals, and check their account balances at any time without the need of human teller.

3. ATM is not a computer by itself and it is connected to a computer that performs the tasks requested by the person using ATM's. The computer is connected electronically to many ATM's that may be located from some distance from the computer.

Decision of the court

ATMs are not computers, but are electronic devices under the Karnataka Sales Tax Act, 1957

7. Place of Electronic Contract

P.R. Transport Agency vs. Union of India & others

AIR2006All23, 2006(1)AWC504

IN THE HIGH COURT OF ALLAHABAD

Civil Misc. Writ Petition No. 58468 of 2005
Decided On: 24.09.2005

Appellants: P.R. Transport Agency through its partner Sri Prabhakar Singh Vs.
Respondent: Union of India (UOI) through Secretary, Ministry of Coal, Bharat Coking Coal Ltd. through its Chairman, Chief Sales Manager Road Sales, Bharat Coking Coal Ltd. and Metal and Scrap Trading Corporation Ltd. (MSTC Ltd.) through its Chairman cum Managing Director

Background of the case

Bharat Coking Coal Ltd (BCC) held an e-auction for coal in different lots. P.R. Transport Agency's (PRTA) bid was accepted for 4000 metric tons of coal from Dobari Colliery.

The acceptance letter was issued on 19th July 2005 by e-mail to PRTA's e-mail address. Acting upon this acceptance, PRTA deposited the full amount of Rs. 81.12 lakh through a cheque in favour of BCC. This cheque was accepted and encashed by BCC.

BCC did not deliver the coal to PRTA. Instead it e-mailed PRTA saying that the sale as well as the e-auction in favour of PRTA stood cancelled "due to some technical and unavoidable reasons".

The only reason for this cancellation was that there was some other person whose bid for the same coal was slightly higher than that of PRTA. Due to some flaw in the computer or its programme or feeding of data the higher bid had not been considered earlier.

This communication was challenged by PRTA in the High Court of Allahabad. [Note: Allahabad is the state of Uttar Pradesh (UP)]

BCC objected to the "territorial jurisdiction" of the Court on the grounds that no part of the cause of action had arisen within U.P.

Issue raised by BCC

The High Court at Allahabad (in U.P.) had no jurisdiction as no part of the cause of action had arisen within U.P.

Issues raised by PRTA

1. The communication of the acceptance of the tender was received by the petitioner by e-mail at Chandauli (U.P.). Hence the contract (from which the dispute arose) was completed at Chandauli (U.P). The completion of the contract is a part of the "cause of action'.

2. The place where the contract was completed by receipt of communication of acceptance is a place where 'part of cause of action' arises.

Points considered by the court

1. In reference to contracts made by telephone, telex or fax, the contract is complete when and where the acceptance is received. However, this principle can apply only where the transmitting terminal and the receiving terminal are at fixed points.

2. In case of e-mail, the data (in this case acceptance) can be transmitted from any where by the e-mail account holder. It goes to the memory of a 'server' which may be located anywhere and can be retrieved by the addressee account holder from anywhere in the world. Therefore, there is no fixed point either of transmission or of receipt.

3. Section 13(3) of the Information Technology Act has covered this difficulty of “no fixed point either of transmission or of receipt”. According to this section “...an electronic record is deemed to be received at the place where the addressee has his place of business."

4. The acceptance of the tender will be deemed to be received by PRTA at the places where it has place of business. In this case it is Varanasi and Chandauli (both in U.P.)

Decision of the court

1. The acceptance was received by PRTA at Chandauli / Varanasi. The contract became complete by receipt of such acceptance.

2. Both these places are within the territorial jurisdiction of the High Court of Allahabad. Therefore, a part of the cause of action has arisen in U.P. and the court has territorial jurisdiction.