CRIME IN CYBERSPACE

First Draft of International Convention Released for Public Discussion

STRASBOURG, 27.04.2000 1 The COUNCIL OF EUROPE today released a draft version of a Convention on crime in cyberspace for public discussion in order to enhance the consultation process with interested parties, whether public or private. Businesses and associations are particularly encouraged to share their comments with the experts involved in the negotiations before the final adoption of the text.

Provisionally entitled "Draft Convention on Cyber-Crime", this Council of Europe text will be the first international treaty to address criminal law and procedural aspects of various types of offending behaviour directed against computer systems, networks or data as well as other similar abuses.

This legally-binding text aims to harmonise national legislation in this field, facilitate investigations and allow efficient levels of co-operation between the authorities of different States.

The text should be finalised by a group of experts by December 2000 and the Committee of Ministers could adopt the text and open it for signature as early as Autumn 2001.
The text of the draft Convention can be found on the following website: http://conventions.coe.int/treaty/en/projet/cybercrime.htm

More information for editors:

Recent attacks against commercial web-sites, such as Amazon.com, drew international attention to the dangers that the Internet and other computer networks need to face: cyber-criminals and cyber-terrorists threaten business and government interests and may cause colossal damages. Time has come for the Council of Europe to take action, which today released a draft Convention to deal with crime in cyberspace. This document, provisionally entitled "Draft Convention on Cyber-crime", will be the first ever international treaty to address criminal law and procedural aspects of various types of criminal behaviour directed against computer systems, networks or data and other types of similar misuse.

The draft provides, among others, for the co-ordinated criminalisation of computer hacking and hacking devices, illegal interception of data and interference with computer systems, computer-related fraud and forgery. It also prohibits on-line child pornography, including the possession of such material after downloading, as well as the reproduction and distribution of copyright protected material. The draft Convention will not only define offences but will also address questions related to the liability of individual and corporate offenders and determine minimum standards for the applicable penalties.

The draft text also deals with law enforcement issues: future Parties will be obliged to empower their national authorities to carry out computer searches and seize computer data, require data-subjects to produce data under their control, preserve or obtain the expeditious preservation of vulnerable data by data-subjects. The interception of data transmitted through networks, including telecommunication networks, is also under discussion. These computer-specific investigative measures will also imply cooperation by telecom operators and Internet Service Providers, whose assistance is vital to identify computer criminals and secure evidence of their misdeeds.

As computer-crimes are often international in their nature, national measures need to be supplemented by international co-operation. The draft treaty therefore requires future Parties to provide each other various forms of assistance, for example by preserving evidence and locating on-line suspects. The text also deals with certain aspects of trans-border computer searches. Traditional forms of mutual assistance and extradition would also be available under the draft Convention and a network of 24 hours/day, 7 days/week available national contact points would be set up to speed up international investigations.

The 41-nation Council of Europe has previously produced two recommendations on the question, in 1989 and in 1995, to encourage governments to adapt laws to the challenge of computer-related crime, but later a binding legal instrument was considered necessary to harmonise computer-crime provisions, step up investigations and ensure effective international co-operation among authorities. The draft Convention is expected to be finalised by an expert group by December 2000 and the Committee of Ministers could adopt the text and open it for signature as early as September 2001. Given the importance of the subject, non-member States, such as Canada, Japan, South-Africa and the United States, also actively participate in the negotiations.

By releasing the latest draft of the treaty, the Council of Europe seeks to enhance the consultation process with interested parties, whether public or private. It particularly encourages business and civil society organisations to come forward and share their comments with the experts involved in the negotiations before the text eventually becomes final."
Commentaries are welcome on: daj@coe.int

Strasbourg, 25 April 2000


EUROPEAN COMMITTEE ON CRIME PROBLEMS (CDPC)

COMMITTEE OF EXPERTS ON CRIME IN CYBER-SPACE (PC-CY)

Draft Convention on Cyber-crime (Draft N° 19)

Prepared by the Secretariat Directorate General I (Legal Affairs)

DRAFT CONVENTION ON CYBER-CRIME (Draft N° 19)

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States signatories to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cyber-crime, inter alia by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned at the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Believing that an effective fight against cyber-crime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as the misuse of such systems, networks and data, by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating the detection, investigation and prosecution of such criminal offences at both the domestic and international level, and by providing arrangements for fast and reliable international co-operation, while ensuring a proper balance between the interests of law enforcement and respect for fundamental human rights.

Welcoming recent developments which further advance international understanding and co-operation in combating cyber-crimes, including actions of the United Nations, the OECD, the European Union and the G8;

Recalling Recommendation N° R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and Recommendation N° R (95) 13 concerning problems of criminal procedural law connected with Information Technology, calling for, inter alia, the negotiation of an international agreement to regulate trans-border search and seizure;
Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, June 1997), which recommended the Committee of Ministers to support the work carried out by the European Committee on Crime Problems (CDPC) on cyber-crime in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation concerning such offences;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe, on the occasion of their Second Summit (Strasbourg, 10 - 11 October 1997), to seek common responses to the development of the new information technologies, based on the standards and values of the Council of Europe;

Have agreed as follows:

CHAPTER I - USE OF TERMS

Article 1 - Definitions (1)

For the purposes of this Convention:

(d) "computer system" means any device or a group of inter-connected devices, which pursuant to a program performs automatic processing of data [or any other function] (2);

(b) "computer data" means:

- any representation of facts, information or concepts in a form suitable for processing in a computer system, or

- set of instructions suitable to cause a computer system to perform a function (3);

(c) "service provider" means any public or private entity that provides to users of its services the ability to send or receive electronic communications;

(d) "traffic data" means:

1. a code indicating a network, equipment or individual number or account, or similar identifying designator, transmitted to or from any designated point in the chain of communication;

2. the time, date, size, and duration of a communication;

3. as to any mode of transmission (including but not limited to mobile transmissions), any information indicating the physical location to or from which a communication is transmitted;

(a) "subscriber data" (4) means:

- any information possessed by the service provider necessary to identify and determine the physical address of a subscriber, user, or account-payer of a service provider’s communications services, and

- any information associated with such subscriber, user, or account-payer possessed by the service provider relating to a network, equipment or individual number or account or similar identifying designators, services, fees; the physical location of equipment, (5) if known and if different from the location information provided under the definition of traffic data;

CHAPTER II - MEASURES TO BE TAKEN AT THE NATIONAL LEVEL

Section 1 - Substantive criminal law
Title 1 - Offences against the confidentiality, integrity and availability of computer data and systems

Article 2 - Illegal Access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally (6) the access to the whole or any part of a computer system without right. A Party may require that the offence be committed either by infringing security measures or with the intent of obtaining computer data or other dishonest intent.

Article 3 - Illegal Interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the interception without right, made by technical means, of non-public (7) transmissions of computer data to, from or within a computer system, as well as electromagnetic emissions from a computer system carrying such computer data.

Article 4 - Data Interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the damaging, deletion, deterioration, alteration (8) or suppression (9) of computer data without right (10).

Article 5 - System Interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 - Illegal Devices

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right:

(a) the production, sale, procurement for use, import, distribution or otherwise making available of:

1. a device, including a computer program, designed or adapted [specifically] [primarily] [particularly] for the purpose of committing any of the offences established in accordance with Article 2 - 5;

2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing the offences established in Articles 2 - 5;

(a) the possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing the offences established in Articles 2 - 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

TITLE 2 - COMPUTER-RELATED OFFENCES

Article 7 - Computer-related Forgery

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally
and without right the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require by law an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related Fraud

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

(a) any input, alteration, deletion or suppression of computer data,

(b) any interference with the functioning of a computer [program] or system, with the intent of procuring, without right, an economic benefit for himself or for another.

Title 3 - Content-related offences

Article 9 - Offences related to child pornography

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed without right and intentionally the following conduct:

(a) offering, distributing, transmitting or [otherwise] making available child pornography through a computer system;

(b) producing child pornography for the purpose of its distribution through a computer system;

(c) possessing child pornography in a computer system or on a data carrier.

2. For the purpose of paragraph 1 above “child pornography” shall include pornographic material that visually depicts:

(a) a minor engaged in a sexually explicit conduct;

(b) a person appearing to be a minor engaged in a sexually explicit conduct;

(c) realistic images representing a minor engaged in a sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term “minor” is to be defined by each Party, but shall include in any case all persons under 14 years of age.

Title 4 – Copyright and related offences

Article 10 - Copyright and related offences

1. Each Party shall adopt such necessary legislative and other measures as may be necessary to establish as criminal offences under its domestic law the reproduction and distribution, by means of a computer system, of works protected by copyright, as defined under the law of that Party, in conformity with the Berne Convention for the Protection of Literary and Artistic Works, the TRIPS Agreement and the WIPO Copyright Treaty, where such acts are committed intentionally on a commercial scale, without right.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the reproduction, distribution
or similar acts, by means of a computer system, of works, items or equivalent creations protected by neighbouring rights, as defined under the law of that Party [in conformity with the WIPO Performances and Phonograms Treaty], where such acts are committed intentionally on a commercial scale, without right.

Title 5 – Ancillary liability and sanctions

Article 11 – Attempt and aiding and abetting

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally:

(a) attempt to commit any of the offences established in accordance with Articles [...] (19)

(b) aiding or abetting (20) the commission of any of the offences established in accordance with Articles 2 – 10 above.

Article 12 – Corporate liability

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for the criminal offences established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

• a power of representation of the legal person; or
• an authority to take decisions on behalf of the legal person; or
• an authority to exercise control within the legal person;
• as well as for involvement of such a natural person as aider or abettor, under Article 11, in the above-mentioned offences.

2. Apart from the cases already provided for in paragraph 1, each Party shall take the necessary measures to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of the criminal offences mentioned in paragraph 1 for the benefit of that legal person by a natural person under its authority.

3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators, aiders or abettors of the criminal offences mentioned in paragraph 1.

Article 13 – Sanctions and measures

1. Each Party shall take the necessary measures to ensure that the criminal offences established in accordance with Articles 2 – 11 are punishable by effective, proportionate and dissuasive sanctions and measures. In particular, each Party shall ensure that the offences established in accordance with Articles [...] (27) and those referred to in Article 21, paragraph 1, when committed by natural persons, are punishable by penalties involving deprivation of liberty which can give rise to extradition.

2. Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Section 2 – Procedural law

Article 14 – Search and Seizure of Stored Computer Data

1. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
(a) a computer system or part of it and computer data stored therein; or
(b) a medium in which computer data may be stored

[in its territory or other place over which it exercises its sovereign powers] (22) for the purposes of criminal investigations or proceedings.

2. Each Party shall take such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, using the measures referred to in paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory or other place over which it exercises its sovereign powers, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. [If the computer system or a part thereof or computer data accessed according to paragraphs 1 or 2 are found out to be inadvertently accessed in the jurisdiction of another Party, the competent authorities of the Party conducting the investigation shall act as provided for in article [...] (23)

4. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2 in view of their possible use in criminal investigations and proceedings. These measures shall include the power to:

(a) seize or similarly secure a computer system or part of it or a medium in which computer data may be stored;
(b) make and retain a copy of those computer data;
(c) maintain the integrity of the relevant stored computer data;
(d) render inaccessible or remove those computer data in the accessed computer system.

5. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to order for the purposes of criminal investigations and proceedings any person who has knowledge about the functioning of the computer system or measures applied to secure the computer data therein to provide all necessary information, as is reasonable, to enable the undertaking of the measures referred to in paragraphs 1 and 4.

6. Where measures referred to in paragraphs 1 and 2 have been taken in respect of a computer system or part of it, or computer data stored therein, the person in charge of (24) the computer system shall as soon as reasonably practicable be duly informed about the executed measures.

7. The powers and procedures referred to in the present Article shall be subject to conditions and safeguards as provided for under national law.

Article 15 - Production Order

1. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to order a person in its territory or other place over which it exercises its sovereign powers to submit specified computer data under this person's control stored in a computer system or a medium (23) in which data may be stored in the form required by these authorities for the purposes of criminal investigations and proceedings.

2. The power referred to in paragraph 1 of the present Article shall be subject to conditions and safeguards as provided for under national law.
Article 16 - Expedited preservation of data stored in a computer system

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or otherwise obtain, for the purpose of criminal investigations or proceedings, the expeditious preservation of data that is stored by means of a computer system, at least where there are grounds to believe that the data is subject to a short period of retention or is otherwise particularly vulnerable to loss or modification.

Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that data for a period of time as may be ordered pursuant to national law.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige a person to whom the procedures of preservation referred to in this Article are directed, to keep confidential the undertaking of such procedures for a period of time as permitted by national law.

4. The powers and procedures referred to in the present article shall be subject to conditions and safeguards as provided for under national law.

Article 17 - Expedited preservation and disclosure of traffic data

1. Each Party shall, with respect to undertaking the procedures referred to under Article 16 in respect of the preservation of traffic data concerning a specific communication, adopt such legislative or other measures as may be necessary to:

(a) ensure the expeditious preservation of that traffic data, regardless whether one or more service providers were involved in the transmission of that communication; and

(b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data in order to identify the service providers and the path through which the communication was transmitted.

2. The powers and procedures referred to in the present article shall be subject to conditions and safeguards as provided for under national law.

Article 18 - Interception (under discussion)

Section 3 - Jurisdiction

Article 19 - Jurisdiction

1. Each Party shall take such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 - 11 of this Convention, when the offence is committed

(a) [in whole or in part] in its territory or on a ship, an aircraft, or a satellite (26) flying its flag or registered in that Party;

(b) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right not to apply
or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraph 1 b of this article or any part thereof.

3. If a Party has made use of the reservation possibility provided for in paragraph 2 of this article, it shall adopt such measures as may be necessary to establish jurisdiction over a criminal offence referred to in Article 21, paragraph 1 of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him to another Party, solely on the basis of his nationality, after a request for extradition.

4. This Convention does not exclude any criminal jurisdiction exercised in accordance with national law.

5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

CHAPTER III – INTERNATIONAL CO-OPERATION

Article 20 - General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and national laws, to the widest extent possible for the purposes of investigations and proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence.

Article 21 - Extradition

The criminal offences established in accordance with Articles 3 - 5 and 7 - 11 of this Convention shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them. With respect to the criminal offence established by Article 2, the following criteria may be required for qualifying that offence as extraditable:

- [the access without right must be made with the intent to breach the confidentiality of data or impair the integrity or availability of data or a computer system, or]
- [the access without right must impair the integrity or availability of data or a computer system.]

2. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this Article.

3. Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this Article as extraditable offences between themselves.

4. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

5. If extradition for a criminal offence referred to in paragraph 1 of this Article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall
submit the case to its competent authorities for the purpose of prosecution unless otherwise agreed with the requesting Party, and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision in the same manner as in the case of any other offence of a comparable nature under the law of that State.

6. (a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty. [Designation of an authority shall not exclude the possibility of using the diplomatic channel.] (27)

(b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Article 22 - Mutual Assistance

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations and proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence.

2. Each Party shall also adopt such legislative or other measures as may be necessary to carry out the obligations set forth in Articles 24 - 29.

3. For the purpose of providing cooperation under articles 24 - 29, each Party shall, in urgent circumstances, accept and respond to mutual assistance requests by expedited means of communications, including [voice], fax or e-mail, to the extent that such means provide appropriate levels of security and authentication, with formal confirmation to follow where required by the requested State.

4. Except as otherwise specifically provided in Articles articles 24 - 29, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse cooperation. (28)

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offense by the same terminology as the requesting Party, if the conduct underlying the offense for which assistance is sought is a criminal offense under its laws.

Article 23 - Procedures pertaining to mutual assistance requests

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, or the Parties concerned do not have national laws under which to provide mutual assistance to one another, the provisions of paragraphs 2 through 10 of this article shall apply. The provisions of this article shall not apply where such agreement, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this Article in lieu thereof.

2. (a) Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.
488

(b) The central authorities shall communicate directly with each other.

(c) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.

(d) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this Article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party. (29)

4. The requested Party may, in addition to conditions or grounds for refusal available under Article 22 (4), refuse assistance if it believes that compliance with the request would prejudice its sovereignty, security, ordre public or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice investigations, prosecutions or related proceedings by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. (a) Without prejudice to its own investigations or proceedings, a Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for cooperation by that Party under this chapter.

(b) Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

9. (a) The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

(b) The requesting Party may request that the requested Party not, without the prior consent of the requesting Party, make use of the substance of the request, nor of the information obtained pursuant to having executed the request, for purposes other than those for which it was obtained or for criminal investigations and related proceedings. If the requested Party cannot comply with the request, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
(c) The requested Party may request that the requesting Party not, without the prior consent of the requested Party, transmit or use the materials furnished for investigations or proceedings other than those stated in the request. If the requested Party accepts the materials subject to the conditions, it shall be bound by them. If the requesting Party cannot comply with the conditions, it shall promptly inform the requesting Party, which shall then determine whether the materials should nevertheless be provided.

10. (a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities, including public prosecutors, of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

(b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

(c) Where a request is made pursuant to subparagraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

(d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

(e) Each Party may, at the time of signature or when depositing its instrument of ratification, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 24 - Provisional measures: Expedited preservation of stored computer data

1. A Party may request another Party to order or otherwise obtain the expedited preservation of data stored by means of a computer system, which is located within the territory of that other Party [or other places over which it exercises its sovereign powers] and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:
   (a) the authority that is seeking the preservation;
   (b) the offence under investigation and a brief summary of related facts;
   (c) the stored data to be preserved and its relationship to the offence;
   (d) the necessity of the preservation;
   (e) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required (30) as a condition to providing such preservation, but may be required as a condition for the disclosure of the data to the requesting Party.
4. A request for preservation as described in paragraph 2 may only be refused if the requested Party believes that compliance with the request would prejudice its sovereignty, security, ordre public or other essential interests.

5. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

6. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 40 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Article 25 - Expedited disclosure of preserved traffic data

1. Where, in the course of the execution of a request made under Article 24 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in a third State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if the requested Party believes that compliance with the request would prejudice its sovereignty, security, ordre public or other essential interests.

Article 26 - Mutual Assistance Regarding Accessing of Stored Data

1. A Party may request another Party to search or similarly access, seize or similarly secure, or disclose data, stored by means of a computer system, which is located within the territory of the other Party (or other place over which it exercises its sovereign powers), including data that has been preserved pursuant to article 24.

2. Upon receipt of a request referred to in paragraph 1, the requested Party shall execute the request as expeditiously as possible, by:

(a) Where permitted by its domestic law, ratifying or endorsing any judicial or other legal authorisation that was granted in the requesting Party to search or seize the data, thereupon executing the search or seizure and, pursuant to its mutual assistance treaties or laws, as applicable, disclosing any data seized to the requesting Party; or

(b) Responding to the request and disclosing any data seized, pursuant to its mutual assistance treaties or laws, as applicable; or

(c) Using any other method of assistance permitted by its domestic law.

Article 27 - Transborder Access to Stored Data Not Requiring Mutual Legal Assistance

[Notwithstanding anything in this Chapter, a Party may, when acting in accordance with its domestic law (and without obtaining the authorisation of another State or providing notice to another State):

(a) access publicly available (open source) data, regardless of where the data is geographically located;

(b) access or receive stored data located in another State, if the Party [has been in contact with a person located within its territory and] acts in accordance
with the lawful and voluntary consent of a person who has the lawful authority to permit the Party access to, or to disclose to the Party, that data.

Article 28 – Interception
[under discussion]

Article 29 - 24/7 Network
1. Each Party shall designate a point of contact available on a 24 hour, 7 day per week basis in order to ensure the provision of immediate assistance for the purpose of the investigation of criminal offenses related to the use of computer systems and data, or for the collection of electronic evidence of any criminal offense. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out:
   1. providing technical advice;
   2. preservation of data pursuant to Articles 24 and 25; and
   3. the collection of evidence, giving of legal information, and locating of suspects.

2. (a) A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

   (b) If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to coordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available in order to facilitate the operation of the network.

CHAPTER IV – FOLLOW-UP

CHAPTER V – FINAL PROVISIONS

Footnotes:
(1) The Drafting Group agreed at its 10th meeting (February 2000) that most definitions under Article 1 should be placed either in relevant parts of the Convention or in the Explanatory report and accordingly deleted from this Article definition: 1/e to 1/n. The remaining definitions (1/a – 1/e) need to be revised by the DG.

(2) The explanatory report should specify that “computer system” refers to the function of data processing and therefore may include any system that is based on such a function, e.g. telecom systems, and that the “inter-connection” referred to in the definition encompasses radio and logical connections. The Chairman noted that in the jurisdiction provision(s), the PC-CY will have to determine to what extent States will be able to claim jurisdiction over acts occurring in the whole or part of such a “computer system”.

(3) The concept of computer data includes computer programs. The Drafting Group agreed that the Explanatory Report should specify, either under Article 1 or another provision, that a “program” is understood as “data suitable for further processing”.

(4) The explanatory report should clarify that subscriber data does not include traffic data nor the content of any communication.
To

The Director State Crime
Record Bureau, salt Lake
Sector II, Kolkata.

Sir,

I, Sri Niupam Sen, Researcher
Scholar at Burdwan University
Judicial Officer, presently
posted as Judicial Magistrate
First Class, Cooch Behar, came to
visit this Institution for my
Research work (Cyber and
Intellecute Property Crime). I
also wish to issue a credit
for visiting the Institution.

Thank you.

Best Regards,

Niupam Sen

[Signature]

Received copy of
Status report
up and date my return
report.

Niupam Sen

30-12-09
North 24 Pgs:-

1. Bidhannagar (South) PS Case No. 36 dt. 27.03.07 U/S 120B/191/192/197/379/425/465/466/468/469/471/427/475 IPC and 65/66 (1)/66 (2)/67/68/69 I.T. Act and 51 (A) 63 (B) Copy Right Act
2. Bidhannagar (North) PS Case No. 123 dt. 10.09.07 U/S 379 IPC & 65/66 I.T. Act
3. Bidhannagar (South) PS Case No. 114 dt. 29.08.07 U/S 509 IPC & 67 I.T. Act
4. Dum Dum PS Case No. 77 dt. 9.04.08 U/S 420/120B/34 IPC
5. Bidhannagar (North) PS Case No.142 dt. 27.08.08 U/S 420 IPC & 65/67 I.T. Act.

Wide spread awareness programme has been lunched to aware the Police personnel as well as public regarding different types of on line Frauds and its prevention.

Six Cases has been registered of this Districts and money involved Rs. 50,000/-.

Already Six (6) Cases is solved.

Kolkata :-

The no of Internet Users who have been victim of Online Cheating during the last three years is 13 (thirteen)

The following steps have been taken by the Govt. to protect people from on line cheating:

Preventive measures have already been taken by implementing Sec.144 Cr.PC in Cyber Cafes and notice have been issued to Cyber Café owners to maintain proper registers for the purpose of verification of identities of the customers.
(1) Various training programmes have already been initiated to create the capability of Police to cope up with Cyber Crimes.
(2) Modern Computers, High-Speed Internet connection, Forensic Tools, Electronic Gadgets etc. have already been supplied to the Units/Divisions of Kolkata Police
(3) Several Computer Awareness Programmes have already been conducted at different Schools, Colleges and other public gatherings to make common people aware of on line cheating.
(4) Cyber Crime Cells and Local Police Stations take prompt and fruitful actions to all reported Cyber cheatings.

1. New Market PS Case No.42 dt. 23.03.06 U/S 120B/420/379 IPC read with 4/20/25 I.T Act & 3/6 Indian Wireless Telegraph Act.
2. Hare Street PS Case No. 243 dt. 19.07.06 U/S 120B/425/467/468/472 IPC
3. Battala PS Case No. 130 dt. 07.08.06 U/S 120B/420 IPC, Rs. 5 Lakhs
4. Hare Street PS Case No. 269 dt. 08/08/06 U/S 120B/420 IPC, Rs. 14375/-
5. Battala PS Case No.150 dt. 31/08/06 U/S 120B/420 IPC, Rs.50000/-
6. Girish Park PS Case No. 84 dt. 01.09.07 U/S 120B/420 IPC, Rs. 47881/-
7. Ultadanga PS Case No. 30 dt. 22.02.07 U/S 120B/467/469/471 IPC
8. New Alipore PS Case No. 38 dt. 18.04.07 U/S 120B/420/379 IPC
9. Tala PS Case No. 67 dt. 26.12.07 U/S 120/420 IPC, Rs. 43424/-
10. Battala PS Case No. 293 dt. 24.09.08 U/S 120B/420/468/471 IPC, Rs. 46320/-
11. Narkeldanga PS Case No. 56 dt. 07.03.08 U/S 120B/419/420/467/468/471 IPC, Rs. 16190/-
12. Tapsia PS Case No. 51 dt. 26.04.08 U/S 120B/420 IPC, Rs. 17736/-
13. Lake PS Case no. 213 dt. 28.08.08 U/S 425/426/468 IPC read with 43
   (a),(b),(c)/66 I.T. Act, 2000

Out of the aforesaid 13 Cases, 5 Cases have already been solved and charge-sheets have been submitted, 4 cases are under investigation and 2 cases are unsolved (declared FRTs)

To solve the unsolved cases Kolkata Police are undertaking the following measures:
(a) Police are trying to build up better communication with concerned ISPs and various Govt. and Non-Govt. Organizations for the collection of intelligence to apprehend the miscreants
(b) Police are taking strict measures against the Cyber Café Owners who are running their business without proper Registers for their customers

**Darjeeling**:

1. Siliguri PS Case No. 112 (4)/2008 U/S 468/420/120B IPC, R/W Sec. 68/72 I.T. Act. Pending Investigation
VISITOR'S MEMO

Dated 15-12-09

Name: 

Visiting for: 

Time of Visit: 3:00 pm

Office to whom visited: A-102/2

Address: 

Signature of the duty officer: 

Signature of the officer to whom visited: 

Signature of the visitors: 

Whom visited with time: 

Signature of the visitors: 

Signature of the duty officer: 

Occupation: 

Address: 

City: 

P.O.-

Signature of the officers: 

Signature of the duty officer: 

Office to whom visited: 

Time of Visit: 

Visiting for: 

Name: 

Visiting for: 

Time of Visit: 3:00 pm

Office to whom visited: A-102/2

Address: 

Signature of the duty officer: 

Signature of the officer to whom visited: 

Signature of the visitors: 

Whom visited with time: 

Signature of the visitors: 

Signature of the duty officer: 

Occupation: 

Address: 

City: 

P.O.-
Kolkata Police H.Q.
CYBER CRIME SECTION, DD, [WEST BLOCK, 2ND FLOOR]

Visitors Slip

Name: NIRUPAM KAR +1 (M-0)

Address: UDAY PALLY PO MADRAL 24 PGS(N)

No. Meet:

Purpose: Official

------------------------------

Visitor's Sign.

NB: The slip is to be deposited at Out-Gate before leaving Kolkata Police Head Quarters.
Name: NIRUPAM KAR +1 (M-O)
Address: UDAY POLLI, PO-MADRA 24 PGS N
Ph No.: 9007804771

To Meet: MRS. DAMAYANTI SEN (IPS)
Deputy Commissioner of Police (DD)
Purpose: Official

NB: The slip is to be deposited at Out-Gate before leaving Kolkata Police Head Quarters.
<table>
<thead>
<tr>
<th><strong>Name</strong></th>
<th>Bhabani Bhawan</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address</strong></td>
<td>3rd Floor, CID</td>
</tr>
<tr>
<td><strong>Whom to visit</strong></td>
<td>Mrs. Dolly, N.C.</td>
</tr>
<tr>
<td><strong>Purpose of visit</strong></td>
<td>Research</td>
</tr>
<tr>
<td><strong>Date</strong></td>
<td>30-12-09</td>
</tr>
</tbody>
</table>
To whom it may concern

Shri Nirupam Kar, Research scholar under university of Burdwan (posted as Judicial Magistrate, 1st class) has visited Cyber Crime Cell of Criminal Investigation Department, Bhabani Bhawan, Kolkata in October 2008 and also today 30.12.2009 for discussing on his research topic.

R. CHATTERJEE
Dy. Superintendent of Police
C. I. D. West Bengal

30/12/09
FIRST INFORMATION REPORT

First information of a cognizable crime reported under section 154 Cr. P.C. at P.S.

District: A.P. Sub-Div. No.: 68 P.S. No.: Year: 2008

(i) Act: 42. P.C. Sections: 194. (ii) Act: Sections:

(iii) Act: Sections: Other Acts & Sections:


2. Occurrence of Offence : Day: Saturday, Date: 04.10.08, Time: 19.15 h, P.S : 188.

3. Information Received Date: 04.10.08, Time: 19.15 h

4. Type of information : Written / Oral

5. Place of Occurrence : (a) Direction and Distance from P.S: Axis Bank, Airport Branch, Kalkata

(b) In case outside limit of this Police Station, then the name of P.S:

6. Complaint/Informer:

(a) Name: Tapir Gosh (A.P of Branch Head)

(b) Father's / Husband's Name: Not noted

(c) Date / Year of Birth: Not noted

(d) Nationality: Indian

(e) Address: Axis Bank, Airport Branch, Kalkata

7. Details of Known/Suspected/unknown/acquainted with full particulars (Attach separate sheet, if necessary):

1. Mr. Bolaiah, 26/3 Topi, R.K., Kat: 39, A.P.

2. M. Narayana Swami, 40/2, Narada, No. 1318, 1st Floor, Chanderkot, Bally, No. 31, H Road, Opp. Ramabhadra Society, S.

8. Reasons for delay in reporting by the Complaint/Informer:

9. Particulars of properties stolen/involved : (Attach separate sheet, if required):

10. Total value of Properties stolen/involved :

11. Inquest report/UID : Case No., if any :

12. FIR Contents : (Attach separate sheets, if required)

13. Action taken : Since the above report reveals commission of offence(s) u/s...

Registered the case and took up the investigation/directed... by A.K. Gosh, to take up

transferred to P.S... on point of jurisdiction... refer to the...

Committed to be correctly recorded and a copy given to the Complaint/Informer free of cost.
I am bringing the following facts to your notice for proper enquiry and recovery of my money, if possible, and punishment to the guilty who have cheated me to the extent of more than two lakhs fifty-seven thousand rupees:

Case No. 1:

I received an e-mail early February this year from one George Smith, President of Australia lottery Inc. (e-mail ID erikahrosten1@aol.com) who informed me about winning a prize of 200,000 US dollars, and asked me to contact their fiduciary Rev. James Atherton (revjamesatherton@yahoo.com). I believed because Smith quoted the Australian Prime Minister as the patron:

Rev. Atherton asked me to contact Dr. Jacob Moyo Ajekigbe, Manager of the International Remittance / Claims Dept, First Bank PLC, Lagos, Nigeria, who in his turn referred me to Barrister Ben Bruce to get Affidavit of claim. The so-called Barrister gave me Affidavit on payment of $300 (Rs.15886.00). Then I had to pay another $2500.00 (Rs.12,750.00) as International Transfer charge for transfer of the prize cheque to my bank account in Kolkata. In this way they defrauded me of a total $2800 (Rs.144,761.00), and all these payments were made in cash to one NITOSHE AWOMI, their broker, in his State Bank of India account no 30495141670 (in Dimapur, Nagaland, as informed by SBI). The entire amount totalling Rs.144,761 has already been withdrawn.

Since then I have been contacting the so-called Dr. Ajekigbe on his telephone number: +2348032084449. and he has been giving me false assurance all the while, without any sign of the money being deposited.

Case No. 2:

In another case I have been foolish enough to be duped by another gang calling itself UK National Lottery (PO Box 1010, Liverpool L70 1NL, UK) which announced I have won 1,000,000 Pound Sterling in their draw No. 1068. Then one Pinkett Brown, the fiduciary (Tel. 44-7024077764, e-mail notify thomas_pink@hotmail.com) sent one bogus diplomat John Coleman, who through phone no. 91-958055920 asked me on 19.3.09 to deposit Rs.26800.00 in cash in SBI as custom charge in the name of LIANTHANGPU, holder of account number 20013750325, which I did. After that, as per his instruction I deposited in the ICICI Bank, first Rs.46,000.00 in the name of ROSALYN LALLAWMZUAL, account no.017701535377, and then another sum of Rs.40,000.00 in the name of:
12. FIR Contents (Attach separate sheets, if n.)

13. Action taken: Since the above report reveals commission of offence(s) u/s. 

420 IPC.

Registered the case and took up the investigation/directed Superintendent of Police, A.K. Ghosh, to take up the

complaint and directed the case to be transferred to P.S................................ of the point of jurisdiction.

Reported to the

Complainant/Informant and a copy given to the Complaint/Informant free of cost.

Signed:

S.P. Ghosh

Rank: Deputy Inspector General of Police

Number of Case: 20-18

Date: 11/11/18
JONATHAM HINAMTHI, a/c. no.017701555814. The said Coleman again asked for Rs. 300,000.00 to get UN clearance which made me suspicious. To convince me he got a Hindi-speaking man to confirm that the amount is in the RBI, New Delhi. He even sent me an RBI receipt and another letter with UN name for payment of rupees three lakhs. I asked a former student of mine who is now a professor at JNU in New Delhi to meet him, but he refused to meet. my former student.

Since then I have been trying to contact these fellows without any success.

I believed them because they held accounts with the largest banks in India. How comes that these prestigious banks become instruments in the hands of frauds.

I request that steps may kindly be taken to expose these gangs as you have already been doing, and, if possible, retrieve my hard earned money as a teacher.

Yours sincerely,

[Signature]

Harapparam
Sub: Fraudulent transactions on my Citibank Card No 4564 0700 5312 1011.

Respected Sir,

This is to draw your kind attention to the fact that I Surajit Paul, holder of the above mentioned credit card was charged unjustifiably for a fraudulent transaction of Rs 1110.00 on 09.02.09 which was operated by hackers on the internet. On 09.02.09 I received a SMS for OAC request no in afternoon, though I have not requested for it. This OAC no is required to develop a new password or to change password in internet banking/ transaction. I immediately informed Citibank about this matter over phone (No 2288-4653) through my land phone no 2658-5050 at around 4.45 to 5.00 pm. I requested to block the card with immediate effect & the bank executive over phone informed me that at that moment I was liable to pay Rs 1585 for my purchases & I agreed to it that it was my genuine purchases from Sukanto Bastralaya & Big Bazaar. So I was assured that till then no fraudulent transaction has taken place from my account as I have acted promptly to block the card. I also rechecked & confirmed my liabilities to be Rs 1585.00 from their phone banking computerized system at that time and made the payment for the same on 14.02.09.

To my astonishment, at midnight on that day I again received a similar SMS towards OAC request no for this same card. I again called up Citibank at around 1.00 am from my mobile no 9831074588 and informed this whole matter & pointed out that how the SMS was sent for a blocked card. This proves that the card was not blocked in spite of my request on my first phone call regarding this matter which is a great act of negligence for Citibank. On the next day i.e. 10.02.09 an executive from their bank visited my residence & informed me that a transaction of Rs 1110.00 has already been done on 09.02.09 and signed me on a review form for review of these fraudulent charges. He also assured me that this charges will be reversed as I have already informed the bank about this matter & requested to block the card immediately after receiving the first SMS. But on the statement dt 25.02.09 I have been charged for those two transactions of Vodafone payments of Rs 555.00 each. I immediately intimated the bank to reverse the charges & they allowed a provisional credit for the same on 16.03.09 vide their e-mail on the same date.

On 23.03.09 I lodged a police complaint to the D.C.D.D. Lalbazaar regarding this matter after guidance from their bank executive & on 26.03.09 Citibank declared vide e-mail that they are unable to reverse the charges. I again pointed out to the fact vide my e-mail dt 27.03.09 that the transactions were made after my request to block the card for which I can’t be rendered liable & once again requested to credit the charges but they choose to sustain to their previous decision.

I would also like to point out that on February, 2009 my mobile no as per Citibank record is 919903055038 & e-mail id is surajitpaul@yahoo.co.in which were both incorrect. I demanded an explanation from where they got this incorrect information but they failed to provide the same. The interesting part of this fact is that I get regular SMS and e-mail to my original mobile no & e-mail id respectively which are mentioned below.

Contd.........Pg.2
on my Citibank Card No 4564 0700 5312 1011.

To my astonishment, at midnight on that day I again received a similar SMS towards OAC request no for this same card. I again called up Citibank at around 1.00 am from my mobile no 9831074588 and informed this whole matter & pointed out that how the SMS was sent for a blocked card. This proves that the card was not blocked in spite of my request on my first phone call regarding this matter which is a great act of negligence for Citibank. On the next day i.e. 10.02.09 an executive from their bank visited my residence & informed me that a transaction of Rs 1110.00 has already been done on 09.02.09 and signed me on a review form for review of these fraudulent charges. He also assured me that these charges will be reversed as I have already informed the bank about this matter & requested to block the card immediately after receiving the first SMS. But on the statement dt 25.02.09 I have been charged for those two transactions of Vodafone payments of Rs 555.00 each. I immediately intimated the bank to reverse the charges & they allowed a provisional credit for the same on 16.03.09 vide their e-mail on the same date.

On 23.03.09 I lodged a police complaint to the D.C.D.D. Lalbazaar regarding this matter after guidance from their bank executive & on 26.03.09 Citibank declared vide e-mail that they are unable to reverse the charges. I again pointed out to the fact vide my e-mail dt 27.03.09 that the transactions were made after my request to block the card for which I can’t be rendered liable & once again requested to credit the charges but they choose to sustain to their previous decision.

I would also like to point out that on February, 2009 my mobile no as per Citibank record is 919903055038 & e-mail id is surajitpaul@yahoo.co.in which were both incorrect. I demanded an explanation from where they got this incorrect information but they failed to provide the same. The interesting part of this fact is that I get regular SMS and e-mail to my original mobile no & e-mail id respectively which are mentioned below.
Sub : Harassment through Internet

Dear Sir,

I would like to inform you that recently so many people are calling land line phone at my maternal place and searching me. When I have enquired the matter I found that some body has published an advertisement on a web-site un-lawfully stating that I am in search male friend. The person had provide my maternal name of Anjana Bose as well as my nick name Ruma with Tel. No. etc. on the web-site.

I have already inform that matter to Baranagar Police Station on 08.10.09 and awaiting their response for your ready reference please note the web-site advertisement like as follow www.datanta.com/en/women/west-bengal.

I don’t know the stranger who published that advertisement. All of my family member facing harassment everyday. I am in fear as my in-laws are un-aware of that and as you know it will be very difficult to make them understand if they come to know the story.

Therefore I seek your help to find out the stranger who had published the same and punished him/her as per law. I am also requesting you to remove the advertisement from the web-site to avoid the unnecessary harassment facing me & my parents everyday.

Looking forward to get and early response.

Thanking you.

Yours truly,
Please be noted that the concerned entire matter is recorded as a general diary with the Jagacha P.S. Dist. Howrah bearing the Ref. GDE No 855 dated 19.05.09. This is for your perusal at your end.

I am enclosing herewith all the relevant documents for your ready reference and also requesting your benign self to pursue the matter so that the concerned bank credit the disputed charges of Rs 1110.00 to my said account and the actual culprits who hold the Vodafone Nos where the recharges have been credited are taken into custody and oblige.