Budapest Convention and the Information Technology Act

The Convention on Cybercrime adopted in Budapest ("Convention") is the fist and one of the most important multilateral treaties addressing the issue of internet and computer crimes.

Introduction

It was drafted by the Council of Europe along with Canada, Japan, South Africa and the United States of America.[1] The importance of the Convention is also indicated by the fact that adherence to it (whether by outright adoption or by otherwise making domestic laws in compliance with it) is one of the conditions mentioned in the Clarifying Lawful Overseas Use of Data Act passed in the USA (CLOUD Act) whereby a process has been established to enable security agencies of in India and the United States to directly access data stored in each other's territories. Our analysis of the CLOUD Act vis-à-vis India can be found here. It is in continuation of that analysis that we have undertaken here a detailed comparison of the Information Technology Act, 2000 ("**IT Act**") and how it stacks up against the provisions of Chapter I and Chapter II of the Convention.[2]

Before we get into a comparison of the Convention with the IT Act, we must point out the distinction between the two legal instruments, for the benefit of readers from a non legal background. An international instrument such as the Convention on Cybercrime (generally speaking) is essentially a promise made by the States which are a party to that instrument, that they will change or modify their local laws to get them in line with the requirements or principles laid out in said instrument. In case the signatory State does not make such amendments to its local laws, (usually) the citizens of that State cannot enforce any rights that they may have been granted under such an international instrument. The situation is the same with the Convention on Cybercrime, unless the signatory State amends its local laws to bring them in line with the provisions of the Convention, there cannot be any enforcement of the provisions of the Convention within that State.[3] This however is not the case for

India and the IT Act since India is not a signatory to the Convention on Cybercrime and therefore is not obligated to amend its local laws to bring them in line with the Convention.

Although India and the Council of Europe cooperated to amend the IT Act through major amendments brought about vide the Information Technology (Amendment) Act, 2008, India still has not become a signatory to the Convention on Cybercrime. The reasons for this appear to be unclear and it has been suggested that these reasons may range from the fact that India was not involved in the original drafting, to issues of sovereignty regarding the provisions for international cooperation and extradition.[4]

Convention on Cybercrime	Information Technology Act, 2000
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, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Section 43** If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network - (a) accesses or secures access to such computer, computer system or computer network or computer resource **Section 66** If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two **three** years or with fine which may extend to five lakh rupees or with both.

The Convention gives States the right to further qualify the offence of “illegal access” or “hacking” by adding elements such as infringing security measures, special intent to obtain computer data, other dishonest intent that justifies criminal culpability, or the requirement that the offence is committed in relation to a computer system that is connected remotely to another computer system.[5] However, Indian law deals with the distinction by making the act of unathorised access without dishonest or fraudulent intent a civil offence, where the offender is liable to pay compensation. If the same act is done with dishonest and fraudulent intent, it is treated as a criminal offence punishable with fine and imprisonment which may extend to 3 years.

It must be noted that this provision was included in the Act only through the Amendment of 2008 and was not present in the Information Technology Act, 2000 in its original iteration.

Convention on Cybercrime	Information Technology Act, 2000

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 transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.	NA

Although the Information Technology Act, 2000 does not specifically criminalise the interception of communications by a private person. It is possible that under the provisions of Rule 43(a) the act of accessing a "computer network" could be interpreted as including unauthorised interception within its ambit.

The other way in which illegal interception may be considered to be illegal is through a combined reading of Sections 69 (Interception) and 45 (Residuary Penalty) with Rule 3 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 which prohibits interception, monitoring and decryption of information under section 69(2) of the IT Act except in a manner as provided by the Rules. However, it must be noted that section 69(2) only talks about interception by the government and Rule 3 only provides for procedural safeguards for such an interception. It could therefore be argued that the prohibition under Rule 3 is only applicable to the government and not to private individuals since section 62, the provision under which Rule 3 has been issued, itself is not applicable to private individuals.

Convention on Cybercrime	Information Technology Act, 2000
Article 4 – Data interference 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	Section 43 If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network - (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (i) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means; (j) Steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage,

he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. (change vide ITAA 2008)

Section 66

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two **three** years or with fine which may extend to five lakh rupees or with both.

Damage, deletion, diminishing in value and alteration of data is considered a crime as per Section 66 read with section 43 of the IT Act if done with fraudulent or dishonest intention. **While the Convention only requires such acts to be crimes if committed intentionally, however the Information Technology Act requires that such intention be either dishonest or fraudulent only then such an act will be a criminal offence, otherwise it will only incur civil consequences requiring the perpetrator to pay damages by way of compensation.**

It must be noted that the optional requirement of such an act causing serious harm has not been adopted by Indian law, i.e. the act of such damage, deletion, etc. by itself is enough to constitute the offence, and there is no requirement of such an act causing serious harm.

As per the Explanatory Report to the Convention on Cybercrime, "**Suppressing** of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored." Strictly speaking the act of suppression of data in another system is not covered by the language of section 43, but looking at the tenor of the section it is likely that if a court is faced with a situation of intentional/malicious denial of access to data, the court could expand the scope of the term "damage" as contained in sub-section (d) to include such malicious acts.

Convention on Cybercrime	Information Technology Act, 2000
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**.	Section 43 If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network - (e) disrupts or causes disruption of any computer, computer system or computer network; **Explanation** - for the purposes of this section - (i) "Computer Contaminant" means any set of computer instructions that are designed - (a) to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or

(b) by any means to usurp the normal operation of the computer, computer system, or computer network;

(iii) "Computer Virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;

Section 66

If any person, dishonestly, or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to two **three** years or with fine which may extend to five lakh rupees or with both.

The offence of causing hindrance to the functioning of a computer system with fraudulent or dishonest intention is an offence under the IT Act. **While the Convention only requires such acts to be crimes if committed intentionally, however the IT Act requires that such intention be either dishonest or fraudulent only then such an act will be a criminal offence, otherwise it will only incur civil consequences requiring the perpetrator to pay damages by way of compensation.**

The IT Act does not require such disruption to be caused in any particular manner as is required under the Convention, although the acts of introducing computer viruses as well as damaging or deleting data themselves have been classified as offences under the IT Act.

Convention on Cybercrime	Information Technology Act, 2000
Article 6 – Misuse of devices	NA
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:	
a the production, sale, procurement for use, import, distribution or otherwise making available of:	
i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;	
ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and	
b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through	

5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing offences against the confidentiality, the integrity and availability of computer systems or data. While the IT Act does not by itself makes the production, sale, procurement for use, import, distribution of devices designed to be adopted for such purposes, sub-section (g) of section 43 along with section 120A of the Indian Penal Code, 1860 which deals with “conspiracy” could perhaps be used to bring such acts within the scope of the penal statutes.

Convention on Cybercrime	Information Technology Act, 2000

Article 7 – Computer related forgery

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

NA

The acts of deletion, alteration and suppression of data by itself is a crime as discussed above, there is no specific offence for doing such acts for the purpose of forgery. However this does not mean that the crime of online forgery is not punishable in India at all, such crimes would be dealt with under the relevant provisions of the Indian Penal Code, 1860 (Chapter 18) read with section 4 of the IT Act.

Convention on Cybercrime	Information Technology Act, 2000

Article 8 – Computer-related fraud

NA

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

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

b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Just as in the case of forgery, there is no specific provision in the IT Act whereby online fraud would be considered as a crime, however specific acts such as charging services availed of by one person to another (section 43(h), identity theft (section 66C), cheating by impersonation (section 66D) have been listed as criminal offences. Further, as with forgery, fraudulent acts to procure economic benefits would also get covered by the provisions of the Indian Penal Code that deal with cheating.

Convention on Cybercrime	Information Technology Act, 2000
Article 9 – Offences related to child pornography 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a producing child pornography **for the purpose of its distribution** through a computer system; b offering or making available child pornography through a computer system; c distributing or transmitting child pornography through a computer system; d procuring child pornography through a computer system for oneself or for another person; e possessing child pornography in a computer system or on a computer-data storage medium. 2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a a minor engaged in sexually explicit conduct; b a person appearing to be a minor engaged in sexually explicit conduct;	**67 B Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.** Whoever,- (a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct or (b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner or (c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource or (d) facilitates abusing children online or (e) records in any electronic form own abuse or that of others pertaining to sexually explicit act with children, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: Provided that the provisions of section 67, section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting, representation or figure in electronic form- (i) The publication of which is proved to be justified as being for the public good on the ground that such book, pamphlet, paper writing, drawing, painting, representation or figure is in the interest of science, literature, art or learning or other objects of general concern; or

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

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, subparagraphs d and e, and 2, sub-paragraphs b and c.

(ii) which is kept or used for bonafide heritage or religious purposes

Explanation: For the purposes of this section, "children" means a person who has not completed the age of 18 years.

The publishing, transmission, creation, collection, seeking, browsing, etc. of child pornography is an offence under Indian law punishable with imprisonment for upto 5 years for a first offence and upto 7 years for a subsequent offence, along with fine.

It is important to note that bona fide depictions for the public good, such as for publication in pamphlets, reading or educational material are specifically excluded from the rigours of the section, Similarly material kept for heritage or religious purposes is also exempted under this section. Such exceptions are in line with the intent of the Convention, since the Explanatory statement itself states that “The term "pornographic material" in paragraph 2 is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt. Therefore, material having an artistic, medical, scientific or similar merit may be considered not to be pornographic.

Convention on Cybercrime	Information Technology Act, 2000
Article 10 – Offences related to infringements of copyright and related rights 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as define under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	**81 Act to have Overriding effect** The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. Provided that nothing contained in this Act shall restrict any person from exercising any

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.	right conferred under the Copyright Act, 1957 or the Patents Act, 1970

The use of the term "pursuant to the obligations it has undertaken" in both paragraphs makes it clear that a Contracting Party to the Convention is not bound to apply agreements cited (TRIPS, WIPO, etc.) to which it is not a Party; moreover, if a Party has made a reservation or declaration permitted under one of the agreements, that reservation may limit the extent of its obligation under the present Convention.

The IT Act does not try to intervene in the existing copyright regime of India and creates a special exemption for the Copyright Act and the Patents Act in the clause which provides this Act overriding effect. India's obligations under the various treaties and conventions on intellectual property rights are enshrined in these legislations.[6]

Convention on Cybercrime	Information Technology Act, 2000
Article 11 – Attempt and aiding or abetting	**84 B Punishment for abetment of offences**
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.	Whoever abets any offence shall, if the act abetted is committed in consequence of the abetment, and no express provision is made by this Act for the punishment of such abetment, be punished with the punishment provided for the offence under this Act. Explanation: An Act or offence is said to be committed in consequence of abetment, when it is committed in consequence of the instigation, or in pursuance of the conspiracy, or with the aid which constitutes the abetment.
2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c of this Convention. 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.	**84 C Punishment for attempt to commit offences** Whoever attempts to commit an offence punishable by this Act or causes such an offence to be committed, and in such an attempt does any act towards the commission of the offence, shall, where no express provision is made for the punishment of such attempt, be punished with imprisonment of any description provided for the offence, for a term which may extend to one-half of the longest term of imprisonment provided for that offence, or with such fine as is provided for the offence or with both.

As can be seen, both attempts as well as abetment of criminal offences under the IT Act have also been criminalised.

Convention on Cybercrime	Information Technology Act, 2000
Article 12 – Corporate liability	**85 Offences by Companies.**

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:	(1) Where a person committing a contravention of any of the provisions of this Act or of any rule, direction or order made there under is a Company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company as well as the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly:
a a power of representation of the legal person;	**Provided** that nothing contained in this sub-section shall render any such person liable to punishment if he proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.
b an authority to take decisions on behalf of the legal person;	
c an authority to exercise control within the legal person.	(2) Notwithstanding anything contained in sub-section (1), where a contravention of any of the provisions of this Act or of any rule, direction or order made there under has been committed by a company and it is proved that the contravention has taken place with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the contravention and shall be liable to be proceeded against and punished accordingly.
2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.	**Explanation**-
	For the purposes of this section
3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.	(i) "Company" means any Body Corporate and includes a Firm or other Association of individuals; and
4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	(ii) "Director", in relation to a firm, means a partner in the firm.

The liability of a company or other body corporate has been laid out in the IT Act in a manner similar to the Budapest Convention. While, the test to determine the relationship between the legal entity and the natural person who has committed the act on behalf of the legal entity is a little more detailed[7] in the Convention, the substance of the test is laid out in the IT Act as “a person who is in charge of, and was responsible to, the company”.

Convention on Cybercrime	Information Technology Act, 2000
Article 14	NA
1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.	

2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

a the criminal offences established in accordance with Articles 2 through 11 of this Convention;

b other criminal offences committed by means of a computer system; and

c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

i is being operated for the benefit of a closed group of users, and

ii does not employ public communications networks and is not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications.

Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

This is a provision of a general nature that need not have any equivalence in domestic law. The provision clarifies that all the powers and procedures provided for in this section (Articles 14 to 21) are for the purpose of “specific criminal investigations or proceedings”.

Convention on Cybercrime	Information Technology Act, 2000
Article 15 – Conditions and safeguards	NA

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and

procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

This again is a provision of a general nature which need not have a corresponding clause in the domestic law. India is a signatory to a number of international human rights conventions and treaties, it has acceded to the International Covenant on Civil and Political Rights (ICCPR), 1966, International Covenant on Economic, Social and Cultural Rights (ICESCR), 1966, ratified the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), 1965, with certain reservations, signed the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979 with certain reservations, Convention on the Rights of the Child (CRC), 1989 and signed the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment (CAT), 1984. Further the right to life guaranteed under Article 21 of the Constitution takes within its fold a number of human rights such as the right to privacy. Freedom of expression, right to fair trial, freedom of assembly, right against arbitrary arrest and detention are all fundamental rights guaranteed under the Constitution of India, 1950.[8]

In addition, India has enacted the Protection of Human Rights Act, 1993 for the constitution of a National Human Rights Commission, State Human Rights Commission in States and Human Rights Courts for better protection of “human rights” and for matters connected therewith or incidental thereto. Thus, there does exist a statutory mechanism for the enforcement of human rights[9] under Indian law. It must be noted that the definition of human rights also incorporates rights embodied in International Covenants and are enforceable by Courts in India.

Convention on Cybercrime	Information Technology Act, 2000
Article 16 – Expedited preservation of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige	**29 Access to computers and data.** (1) Without prejudice to the provisions of sub-section (1) of section 69, the Controller or any person authorized by him shall, if he has reasonable cause to suspect that any contravention of the provisions of this chapter made there under has been committed, have access to any computer system, any apparatus, data or any other material connected with such system, for the purpose of searching or causing a search to be made for obtaining any information or data contained in or available to such computer system. (Amended vide ITAA 2008) (2) For the purposes of sub-section (1), the Controller or any person authorized by him may, by order, direct any person in charge of, or otherwise concerned with the operation of the computer system, data apparatus or material, to provide him with such reasonable technical and other assistant as he may consider necessary. **67 C Preservation and Retention of information by intermediaries**

the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 17 – Expedited preservation and partial disclosure of traffic data

1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:

a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

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

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

(1) Intermediary shall preserve and retain such information as may be specified for such duration and in such manner and format as the Central Government may prescribe.

Rule 3(7) of the Information Technology (Intermediary Guidelines) Rules, 2011

3(7) - When required by lawful order, the intermediary shall provide information **or any such assistance** to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. The information or any such assistance shall be provided for the purpose of verification of identity, or for prevention, detection, investigation, prosecution, cyber security incidents and punishment of offences under any law for the time being in force, on a request in writing staling clearly the purpose of seeking such information or any such assistance.

It must be noted that Article 16 and Article 17 refer only to data preservation and not data retention. "Data preservation" means to keep data, which already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. Data retention means to keep data, which is currently being generated, in one's possession into the future.[10] In short, the article provides only for preservation of existing stored data, pending subsequent disclosure of the data, in relation to specific criminal investigations or proceedings.

The Convention uses the term "order or similarly obtain", which is intended to allow the use of other legal methods of achieving preservation than merely by means of a judicial or administrative order or directive (e.g. from police or prosecutor). In some States, preservation orders do not exist in the procedural law, and data can only be preserved and obtained through search and seizure or production order. Flexibility was therefore intended by the use of the phrase "or otherwise obtain" to permit the implementation of this article by the use of these means.

While Indian law does not have a specific provision for issuing an order for preservation of data, the provisions of section 29 as well as sections 99 to 101 of the Code of Criminal Procedure, 1973 may be utilized to achieve the result intended by Articles 16 and 17. Although section 67C of the IT Act uses the term "preserve and retain such information", this provision is intended primarily for the purpose of data retention and not data preservation.

Another provision which may conceivably be used for issuing preservation orders is Rule 3(7) of the Information Technology (Intermediary Guidelines) Rules, 2011 which requires intermediaries to provide "any such assistance" to Government Agencies who are lawfully authorised for investigative, protective, cyber security activity. However, in the absence of a power of preservation in the main

statute (IT Act) it remains to be seen whether such an order would be enforced if challenged in a court of law.

Convention on Cybercrime	Information Technology Act, 2000
Article 18 – Production order	
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:	
a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and	
b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.	**Section 28(2)** (2) The Controller or any officer authorized by him in this behalf shall exercise the like powers which are conferred on Income-tax authorities under Chapter XIII of the Income-Tax Act, 1961 and shall exercise such powers, subject to such limitations laid down under that Act.
2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	
3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:	**Section 58(2)** (2) The Cyber Appellate Tribunal shall have, for the purposes of discharging their functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely -
a the type of communication service used, the technical provisions taken thereto and the period of service;	(b) requiring the discovery and production of documents or other electronic records;
b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;	
c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.	

While the Cyber Appellate Tribunal and the Controller of Certifying Authorities both have the power to call for information under the IT Act, these powers can be exercised only for limited purposes since the jurisdiction of both authorities is limited to the procedural provisions of the IT Act and they do not have the jurisdiction to investigate penal provisions. In practice, the penal provisions of the IT Act are investigated by the regular law enforcement apparatus of India, which use statutory provisions for production orders applicable in the offline world to computer systems as well. It is a very common practice amongst law enforcement authorities to issue orders under the Code of Criminal Procedure, 1973 (section 91) or the relevant provisions of the Income Tax Act, 1961 to compel production of

information contained in a computer system. The power to order production of a "document or other thing" under section 91 of the Criminal Procedure Code is wide enough to cover all types of information which may be residing in a computer system and can even include the entire computer system itself.

Convention on Cybercrime	Information Technology Act, 2000
Article 19 – Search and seizure of stored computer data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a a computer system or part of it and computer data stored therein; and b a computer-data storage medium in which computer data may be stored in its territory. 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a seize or similarly secure a computer system or part of it or a computer-data storage medium; b make and retain a copy of those computer data; c maintain the integrity of the relevant stored computer data;	**76 Confiscation** Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provision of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation: **Provided** that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules, orders or regulations made there under, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made there under as it may think fit.

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

4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

5 The powers and procedures referred to in this article shall be subject to Articles 14 and15.

While Article 19 provides for the power to search and seize computer systems for the investigation into criminal offences of any type of kind, section 76 of the IT Act is limited only to contraventions of the provisions of the Act, rules, orders or regulations made thereunder. However, this does not mean that Indian law enforcement authorities do not have the power to search and seize a computer system for crimes other than those contained in the IT Act; just as in the case of Article 18, the authorities in India are free to use the provisions contained in the Criminal Procedure Code and other sectoral legislations which allow for seizure of property to seize computer systems when investigating criminal offences.

Convention on Cybercrime	Information Technology Act, 2000
Article 20 – Real-time collection of traffic data 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a collect or record through the application of technical means on the territory of that Party, and b compel a service provider, within its existing technical capability: i to collect or record through the application of technical means on the territory of that Party; or ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the	**69B Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security** (1) The Central Government may, to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country, by notification in the official Gazette, authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource. (2) The Intermediary or any person in-charge of the Computer resource shall when called upon by the agency which has been authorized under sub-section (1), provide technical assistance and extend all facilities to such agency to enable online access or to secure and provide online access to the computer resource generating , transmitting, receiving or storing such traffic data or information.

measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

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

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

(3) The procedure and safeguards for monitoring and collecting traffic data or information, shall be such as may be prescribed.

(4) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (2) shall be punished with an imprisonment for a term which may extend to three years and shall also be liable to fine.

Explanation: For the purposes of this section, (i) "Computer Contaminant" shall have the meaning assigned to it in section 43.

(ii) "traffic data" means any data identifying or purporting to identify any person, computer system or computer network or location to or from which the communication is or may be transmitted and includes communications origin, destination, route, time, date, size, duration or type of underlying service or any other information.

Section 69B in the IT Act enables the government to authorise the monitoring and collection of traffic data through any computer system. Under the Convention, orders for collection and recording of traffic data can be given for the purposes mentioned in Articles 14 and 15. On the other hand, as per the Information Technology (Procedure and safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009, an order for monitoring may be issued for any of the following purposes relating to cyber security:

(a) forecasting of imminent cyber incidents;

(b) monitoring network application with traffic data or information on computer resource;

(c) identification and determination of viruses or computer contaminant;

(d) tracking cyber security breaches or cyber security incidents;

(e) tracking computer resource breaching cyber security or spreading virus or computer contaminants;

(f) identifying or tracking of any person who has breached, or is suspected of having breached or being likely to breach cyber security;

(g) undertaking forensic of the concerned computer resource as a part of investigation or internal audit of information security practices in the computer resources;

(h) accessing a stored information for enforcement of any provisions of the laws relating to cyber security for the time being in force;

(i) any other matter relating to cyber security.

As can be seen from the above, the reasons for which an order for monitoring traffic data can be issued are extremely wide, this is in stark contrast to the reasons for which an order for interception of content data may be issued under section 69. The Rules also provide that the intermediary shall not disclose the existence of a monitoring order to any third party and shall take all steps necessary to ensure extreme secrecy in the matter of monitoring of traffic data.

Convention on Cybercrime Information Technology Act, 2000

Article 21 – Interception of content data

1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a collect or record through the application of technical means on the territory of that Party, and

b compel a service provider, within its existing technical capability:

i to collect or record through the application of technical means on the territory of that Party, or

ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.

3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the

69 Powers to issue directions for interception or monitoring or decryption of any information through any computer resource

(1) Where the central Government or a State Government or any of its officer specially authorized by the Central Government or the State Government, as the case may be, in this behalf may, if is satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defense of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information transmitted received or stored through any computer resource.

(2) The Procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed

(3) The subscriber or intermediary or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub section (1), extend all facilities and technical assistance to -

(a) provide access to **or secure access to** the computer resource containing such information; generating, transmitting, receiving or storing such information; or

(b) intercept or monitor or decrypt the information, as the case may be**;** or

(c) provide information stored in computer resource.

(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with an imprisonment for a term which may extend to seven years and shall also be liable to fine.

execution of any power provided for in this article and any information relating to it.

4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

There has been a lot of academic research and debate around the exercise of powers under section 69 of the IT Act, but the current piece is not the place for a standalone critique of section 69.[11] The analysis here is limited to a comparison of the provisions of Article 20 vis-à-vis section 69 of the IT Act.

In that background, it needs to be pointed out that two important issues mentioned in Article 20 of the Convention are not specifically mentioned in section 69B, viz. (i) that the order should be only for specific computer data, and (ii) that the intermediary should keep such an order confidential; these requirements are covered by Rules 9 and 20 of the Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, respectively.

Convention on Cybercrime	Information Technology Act, 2000
Article 22 – Jurisdiction 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a in its territory; or b on board a ship flying the flag of that Party; or c on board an aircraft registered under the laws of that Party; or d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its	**1. Short Title, Extent, Commencement and Application** (2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person. **75 Act to apply for offence or contraventions committed outside India** (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. (2) For the purposes of sub-section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention involves a computer, computer system or computer network located in India.

domestic law.

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

The Convention provides for extra territorial jurisdiction only for crimes committed outside the State by nationals of that State. However, the IT Act applies even to offences under the Act committed by foreign nationals outside India, as long as the act involves a computer system or computer network located in India.

Unlike para 3 of Article 22 of the Convention, the IT Act does not touch upon the issue of extradition. Cases involving extradition would therefore be dealt with by the general law of the land in respect of extradition requests contained in the Extradition Act, 1962. The Convention requires that in cases where the state refuses to extradite an alleged offender, it should establish jurisdiction over the offences referred to in Article 21(1) so that it can proceed against that offender itself. In this regard, it must be pointed out that Section 34A of the Extradition Act, 1962 provides that “Where the Central Government is of the opinion that a fugitive criminal cannot be surrendered or returned pursuant to a request for extradition from a foreign State, it may, as it thinks fit, take steps to prosecute such fugitive criminal in India.” Thus the Extradition Act gives the Indian government the power to prosecute an individual in the event that such individual cannot be extradited.

International Cooperation

Chapter III of the Convention deals specifically with international cooperation between the signatory parties. Such co-operation is to be carried out both "in accordance with the provisions of this Chapter" and "through application of relevant international agreements on international cooperation in criminal matters, arrangements agreed to on the basis of uniform or reciprocal legislation, and domestic laws." The latter clause establishes the general principle that the provisions of Chapter III do not supersede the provisions of international agreements on mutual legal assistance and extradition or the relevant provisions of domestic law pertaining to international co-operation.[12] Although the Convention grants primacy to mutual treaties and agreements between member States, in certain specific circumstances it also provides for an alternative if such treaties do not exist between the member states (Article 27 and 28). The Convention also provides for international cooperation on certain issues which may not have been specifically provided for in mutual assistance treaties entered into between the parties and need to be spelt out due to the unique challenges posed by cyber crimes, such as expedited preservation of stored computer data (Article 29) and expedited disclosure of preserved traffic data (Article 30). Contentious issues such as access to stored computer data, real time collection of traffic data and interception of content data have been specifically left by the Convention to be dealt with as per existing international instruments or arrangements between the parties.

Conclusion

The broad language and wide terminology used IT Act seems to cover a number of the cyber crimes mentioned in the Budapest Convention, even though India has not signed and ratified the same. Penal provisions such as illegal access (Article 2), data interference (Article 4), system interference (Article 5), offence related to child pornography (Article 9), attempt and aiding or abetting (Article 11), corporate liability (Article 12) are substantially covered and reflected in the IT Act in a manner very similar to the requirements of the Convention. Similarly procedural provisions such as search and seizure of stored computer data (Article 19), real-time collection of traffic data (Article 20), interception of content data (Article 21) and Jurisdiction (Article 22) are also substantially reflected in the IT Act.

However certain penal provisions mentioned in the Convention such as computer related forgery (Article 7), computer related fraud (Article 8) are not provided for specifically in the IT Act but such

offences are covered when provisions of the Indian Penal Code, 1860 are read in conjugation with provisions of the IT Act. Similarly procedural provisions such as expedited preservation of stored computer data (Article 16) and production order (Article 18) are not specifically provided for in the IT Act but are covered under Indian law through the provisions of the Code of Criminal Procedure, 1973.

Apart from the above two categories there are certain provisions such as misuse of devices (Article 6) and Illegal interception (Article 3) which may not be specifically covered at all under Indian law, but may conceivably be said to be covered through an expansive reading of provisions of the Indian Penal Code and the IT Act. It may therefore be said that even though India has not signed or ratified the Budapest Convention, the legal regime in India is substantially in compliance with the provisions and requirements contained therein.

Thus, the Convention on Cybercrime is perhaps the most important international multi state instruments that may be used to combat cybercrime, not merely because the provisions thereunder may be used as a model to bolster national/local laws by any State, be it a signatory or not (as in the case of India) but also because of the mechanism it lays down for international cooperation in the field of cyber terrorism. In an increasingly interconnected world where more and more information of individuals is finding its way to the cloud or other networked infrastructure the international community is making great efforts to generate norms for increased international cooperation to combat cybercrime and cyber terrorism. While the Convention is one such multilateral effort, States are also proposing to use bilateral treaties to enable them to better fight cybercrime, the United States CLOUD Act, being one such effort. In the backdrop of these novel efforts the role to be played by older instruments such as the Convention on Cybercrime as well as by important States such as India is extremely crucial.

---

[1] Explanatory Report to the Convention on Cybercrime, Para 304, https://rm.coe.int/16800cce5b.

[2] The analysis here has been limited to only Chapter I and Chapter II of the Convention, as it is only adherence to these two chapters that is required under the CLOUD Act.

[3] The only possible enforcement that may be done with regard to the Convention on Cybercrime is that the Council of Europe may put pressure on the signatory State to amend its local laws (if it is refusing to do so) otherwise it would be in violation of its obligations as a member of the European Union.

[4] Alexander Seger, “India and the Budapest Convention: Why Not?”, https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/

[5] Explanatory Report to the Convention on Cybercrime, Para 50, https://rm.coe.int/16800cce5b.

[6] India is a party to the Berne Convention on Literary and Artistic Works, the Agreement on Trade Related Intellectual Property Rights and the Rome Convention. India has also recently (July 4, 2018) announced that it will accede to the WIPO Copyright Treaty as well as the WIPO Performances and Phonographs Treaty.

[7] The test under the Convention is that the relevant person would be the one who has a leading position within the company, based on:

- a power of representation of the legal person;
- an authority to take decisions on behalf of the legal person;
- an authority to exercise control within the legal person.

[8]Vipul Kharbanda and Elonnai Hickock, “MLATs and the proposed Amendments to the US Electronic Communications Privacy Act”, https://cis-india.org/internet-governance/blog/mlats-and-the-proposed-amendments-to-the-us-electronic-communications-privacy-act

[9] The term “human rights” has been defined in the Act as “rights relating to life, liberty, equality and dignity of the individual guaranteed by the Constitution or embodied in the International Covenants and enforceable by courts in India”.

[10] Explanatory Report to the Convention on Cybercrime, Para 151, https://rm.coe.int/16800cce5b. .

[11] A similar power of interception is available under section 5 of the Telegraph Act, 1885, but that extends only to interception of telegraphic communication and does not extend to communications exchanged through computer networks.

[12] Explanatory Report to the Convention on Cybercrime, Para 244, https://rm.coe.int/16800cce5b.

Send this

Filed under: Cyber Security, Internet Governance

Meta

20 November, 2018

Cyber Security, Internet Governance

Author

Vipul Kharbanda

Blog

We need a better AI vision
Oct 14, 2019

AI for Good
Oct 09, 2019

Designing a Human Rights Impact Assessment for ICANN’s Policy Development Processes
Oct 03, 2019

AI: Full Spectrum Regulatory Challenge Launch Workshop [Reference Files]
Oct 01, 2019

Artificial Intelligence: a Full-Spectrum Regulatory Challenge [Working Draft]
Oct 01, 2019

Events

Internet Speech: Perspectives on Regulation and Policy

SOTM Asia 2018

Workshop on Cybersecurity Illustrations

Roundtable on Cyber-security and the Private Sector

Symposium on India's Cyber Strategy

Funded by

kusuma trust

Kusuma Trust

Kusuma Trust supports innovation, new developments in higher education, training and advocacy, all of which have enormous potential to benefit society.

Offices

Bengaluru: No. 194, 2nd 'C' Cross, Domlur, 2nd Stage, Bengaluru, 560071. Location on Google Map. 080 4092 6283.

Delhi: First floor, B 1/8, Hauz Khas, near G Block market, take the gate opposite Southy, New Delhi, 110016. Location on Google Map. 011 4050 3285

Support Us

Please help us defend citizen and user rights on the Internet!

You may donate online via Instamojo. Or, write a cheque in favour of 'The Centre for Internet and Society' and mail it to us at No. 194, 2nd 'C' Cross, Domlur, 2nd Stage, Bengaluru, 560071.

Follow our Works

Newsletter: Subscribe

researchers@work blog: medium.com/rawblog

Twitter (CIS): @cis_india

Twitter (CIS-A2K): @cisa2k

Request for Collaboration

We invite researchers, practitioners, artists, and theoreticians, both organisationally and as individuals, to engage with us on topics related internet and society, and improve our collective understanding of this field. To discuss such possibilities, please write to Sunil Abraham, Executive Director, at sunil[at]cis-india[dot]org or Sumandro Chattapadhyay, Director, at sumandro[at]cis-india[dot]org, with an indication of the form and the content of the collaboration you might be interested in.

In general, we offer financial support for collaborative/invited works only through public calls.

About Us

The Centre for Internet and Society (CIS) is a non-profit organisation that undertakes interdisciplinary research on internet and digital technologies from policy and academic perspectives. The areas of focus include digital accessibility for persons with disabilities, access to knowledge, intellectual property rights, openness (including open data, free and open source software, open standards, open access, open educational resources, and open video), internet governance, telecommunication reform, digital privacy, and cyber-security. The research at CIS seeks to understand the reconfiguration of social processes and structures through the internet and digital media technologies, and vice versa.

Through its diverse initiatives, CIS explores, intervenes in, and advances contemporary discourse and regulatory practices around internet, technology, and society in India, and elsewhere.

- Annual Reports
- Organisational Policies
- Newsletters
- Logos
- People
- Vacancies