The Report of the Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and Implications for India

List of Acronyms

ICTs – Information Communication Technologies

GGE – Group of Experts

EU – European Union

DLC-ICT – India-Belarus Digital Learning Center

IT Act – Information Technology Act, 2000

UL - Unified License

DEITY – Department of Electronics and Information Technology

IT – Information Technology

ISO – International Organization for Standardisation

CERT – Computer Emergency Response Team

CERT-In - Computer Emergency Response Team, India

MLAT – Mutual Legal Assistance Treaty

CII – Critical Information Infrastructure

NCIIPC - National Critical Information Infrastructure Protection Centre

NTRO - National Technical Research Organisation

NPIT - National Policy on Information Technology

CISO - Chief Information Security Officer

INTRODUCTION

Very few technologies in the history of our civilization have been as powerful in reshaping economies, societies and international relations as information and communications technologies

(ICTs). Cyberspace[1] touches every aspect of our lives, has enormous benefits, but is also accompanied by a number of risks. The international community at large has realized that cyberspace can be made stable and secure only through international cooperation. Traditionally, though there are a number of bilateral agreements and forms of cooperation the foundation of this cooperation has been the international law and the principles of the Charter of the United Nations.

To this end, on December 27, 2013 the United Nations General Assembly adopted Resolution No. 68/243 requesting the "*Secretary General, with the assistance of a group of governmental experts,…… to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States……. and to submit to the General Assembly at its seventieth session a report on the results of the study.*" In pursuance of this resolution the Secretary General established a Group of Experts on Developments in the Field of Information and Telecommunications in the Context of International Security; the report was agreed upon by the Group of Experts in June, 2015. On 23 December 2015, the UN General Assembly unanimously adopted resolution 70/237[2] which welcomed the outcome of the Group of Experts and requested the Secretary-General to establish a new GGE that would report to the General Assembly in 2017.

The report developed by governmental experts from 20 States addresses existing and emerging threats from uses of ICTs, by States and non-State actors alike. These threats have the potential to jeopardize international peace and security. The experts gave recommendations which have built on consensus reports issued in 2010 and 2013, and offer ideas on norm-setting, confidence-building, capacity-building and the application of international law for the use of ICTs by States.

[1]The terms "cyberspace" has been defined in the Oxford English Dictionary as the notional environment in which communication over computer networks occurs. Although the scope of this paper is not to discuss the meaning of this term, it was felt that a simple definition of the term would be useful to better define the parameters of the discussion.

[2]https://s3.amazonaws.com/unoda-web/wp-content/uploads/2016/01/A-RES-70-237-Information-Security.pdf

Among other recommendations, the Report lays down recommendations for States for voluntary, non-binding norms, rules or principles of responsible behaviour to promote an open, secure, stable, accessible and peaceful ICT environment.

As larger international dialogues around cross border sharing of information and cooperation for cyber security purposes take place between the US and EU, it is critical that India begin to participate in these discussions.[3] It is also necessary to take cognizance of the importance of implementing internal practices and policies that are recognized and set strong standards at the international level.

This paper marks the beginning of a series of questions we will be asking and processes we will be analysing with the aim of understanding the role of international cooperation for cyber security and the interplay between privacy and security. The report analyses the existing norms in India in the backdrop of the recommendations in the Report of Experts to discover how interoperable Indian law and policy is vis-à-vis the recommendations made in this report as well as making recommendations towards ways India can enhance national policies, practices, and approaches to enable greater collaboration at the international level with respect to issues concerning ICTs and security.

[3]https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/

ANALYSIS OF THE RECOMMENDATIONS

The Group of Experts took into account existing and emerging threats, risks and vulnerabilities, in the field of ICT and offered the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour:

(a) Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security;

1. India has been working with a number of countries such as Belarus, Canada, China, Egypt, and France on a number of ICT-related isues thereby increasing international cooperation in the ICT sector, such as:

(i) setting up the India-Belarus Digital Learning Centre (DLC-ICT) to promote

development of ICT in Belarus;

(ii) sending an official business delegation to Canada to attend the 2nd Joint Working Group meeting in ICTE;

(iii) holding Joint Working Groups on ICT with China.[4]

As can be seen from this, most of the cooperation with other countries is currently government to government (or government institution to government institution) cooperation. However, it must be noted that the entire digital revolution, including ICT necessarily involves ICT companies, and thus the role of the private sector in participating in these negotiations as well as the responsibilities of private sector ICT companies in cross border cooperation. Furthermore, the above examples are a few of the many agreements, Memoranda of Understanding (MOU), and negotiations that India has with other countries on cross border cooperation. It is important that, to the extent possible, these negotiations and transparent and easily publicly available.

[4] http://deity.gov.in/content/country-wise-status

2. The primary legislation governing ICT in India is the Information Technology Act, 2000 ("IT Act") which was passed to provide legal recognition for the transactions carried out by means of electronic data interchange and other means of electronic communication. The IT Act contains a number of provisions that declare illegal activities that threatenICT infrastructure, data, and individuals as illegal and provide for penalties for the same. These activities are:

Section 43 - *Penalty and Compensation for damage to computer, computer system, etc.:* If any person without permission: (i) accesses a computer, computer system or network; (ii) downloads, copies or extracts any data from such computer, computer system or network; (iii) introduces any computer contaminant or computer virus into, destroys, deletes or alters any information on, damages or disrupts any computer, computer system or network; (iv) denies or causes the denial of access to any computer, computer system or network by any means; (v) helps any person to access a computer, computer system or network in contravention of the Act; (vi) charges the services availed of by a person to the account of another person through manipulation; or (vii) 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 to the person so affected.

Section 66 - *Computer Related Offences:* 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 Rs. 5,00,000/- or with both.

Section 66B - *Punishment for dishonestly receiving stolen computer resource or communication device:*Whoever dishonestly receives or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to Rs. 1,00,000/- or with both.

Section 66C - *Punishment for identity theft:*Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which

may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D - *Punishment for cheating by personation by using computer resource:*Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to Rs. 1,00,000/- .

Section 66E - *Punishment for violation of privacy:*Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding Rs. 2,00,000 or with both.

Section 66F - *Punishment for cyber terrorism:*(1) Whoever,- (A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by –

- denying or cause the denial of access to computer resource; or
- attempting to penetrate a computer resource; or
- introducing or causing to introduce any computer contaminant and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure, or

(B) knowingly or intentionally penetrates a computer resource and by by doing so obtains access to information that is restricted for reasons of the security of the State or foreign relations; or any restricted information with reasons to believe that such information may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise, commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.

Section 67 - *Publishing of information which is obscene in electronic form:* Whoever publishes or transmits in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons, shall be punished on first conviction with a maximum imprisonment upto 2 years and a maximum fine upto Rs. 5,00,000 and for a second or subsequent conviction with a maximum imprisonment upto 5 years and also a maximum with fine upto Rs. 10,00,000.

Section 67A - *Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form:*Whoever publishes or transmits in the electronic form any material which contains sexually explicit act or conduct shall be punished on 1st conviction with a maximum imprisonment for 5 years and a maximum fine of upto Rs. 10,00,000 and for a 2nd or subsequent conviction with a maximum imprisonment of 7 years and a maximum fine upto Rs. 10,00,000.

Section 67B - *Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form:* Whoever,- (a) publishes or transmits 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 a maximum imprisonment upto 5 years and a maximum fine upto Rs. 10,00,000 and in the event of a 2nd or subsequent conviction with a maximum imprisonment upto 7 years and also a maximum fine upto Rs. 10,00,000.[5]

Section 72 - *Breach of confidentiality and privacy:* Any person who, in pursuance of any of the powers conferred under this Act, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses the same to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to Rs. 1,00,000 or with both.

Section 72-A - *Punishment for Disclosure of information in breach of lawful contract:* Any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to Rs. 5,00,000 or with both.

---

[5]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

(ii) which is kept or used for *bona fide* heritage or religious purposes

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

3. The broad language and wide terminology used IT Act seems to cover most of the cyber crimes faced in India as of now, though the technical abilities to prevent the crimes still leave a lot to be desired. The prevention of cyber crime is not the domain of the IT Act and is rather the responsibility of the law enforcement authorities (note: there is no specific authority created under the IT Act, the Act is enforced by the police and other law enforcement authorities). That said, it may be a useful exercise to briefly compare these provisions with the crimes mentioned in the Convention on Cybercrime, 2001 (Budapest Convention), an international treaty that seeks to addresses threats in cyber space by promoting the harmonization of national laws and cooperation across jurisdictions, to examine if there are any that are not covered by the IT Act. A comparison of the principles in Budapest Convention and the IT Act is below:

S. No.	Article of the Budapest Convention	Provisions of the IT Act which cover the same
1	Article 2 - Illegal Access	Section 43(a) read with Section 66
2	Article 3 - Illegal Interception	Section 69 of the IT Act read with section 45 as well as Section 24 of the Telegraph Act, 1885
3	Article 4 - Data interference	Sections 43(d) and 43(f) read with section 66
4	Article 5 - System interference	Sections 43(d), (e) and (f) read with section 66
5	Article 6 - Misuse of devices	Not specifically covered
6	Article 7 - Computer related forgery	Computer related forgery is not specifically covered, but it is possible that when such a case comes to light, the provisions of Section 43 read with section 66 as well as provisions of the Indian Penal Code, 1860 would be pressed into service to cover such crimes
7	Article 8 - Computer related fraud	While not specifically covered by the IT Act, it is possible that when such a case comes to light, the provisions of Section 43 read with section 66 as well as provisions of the Indian Penal Code, 1860 would be pressed into service to cover such crimes
8	Article 9 - Offences relating to child pornography	Section 67B

As can be seen from the above discussion, most of the criminal acts elucidated in the Budapest Convention are covered under the IT Act except for the provision on misuse of devices, which requires the production, dealing, trading, etc. in devices whose sole objective is to violate the

provisions of the IT Act, though it is possible that provisions of the Indian Penal Code, 1860 dealing with conspiracy and aiding and abetment may be pressed into service to cover such incidents.

4. Further, there are a number of laws which deal with critical infrastructure in India, however since these are mostly sectoral laws dealing with specific infrastructure sectors, the one most relevant to ICT is the Telegraph Act, 1885, which makes it illegal to interfere with or damage critical telegraph infrastructure. The specific penal provisions are listed below:

> **Section 23 -** *Intrusion into signal-room, trespass in telegraph office or obstruction:* If any person - (a) without permission of competent authority, enters the signal room of a telegraph office of the Government, or of a person licensed under this Act, or (b) enters a fenced enclosure round such a telegraph office in contravention of any rule or notice not to do so, or (c) refuses to quit such room or enclosure on being requested to do so by any officer or servant employed therein, or (d) wilfully obstructs or impedes any such officer or servant in the performance of his duty, he shall be punished with fine which may extend to Rs. 500.
>
> **Section 24** - *Unlawfully attempting to learn the contents of messages:* If any person does any of the acts mentioned in section 23 with the intention of unlawfully learning the contents of any message, or of committing any offence punishable under this Act, he may (in addition to the fine with which he is punishable under section 23) be punished with imprisonment for a term which may extend to one year.
>
> **Section 25** - *Intentionally damaging or tampering with telegraphs:* If any person, intending – (a) to prevent or obstruct the transmission or delivery of any message, or (b) to intercept or to acquaint himself with the contents of any message, or (c) to commit mischief, damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other thing whatever, being part of or used in or about any telegraph or in the working thereof, he shall be punished with imprisonment for a term which may extend to three years, or with fine or with both.

Section 25A - *Injury to or interference with a telegraph line or post:* If, in any case not provided for by section 25, any person deals with any property and thereby wilfully or negligently damages any telegraph line or post duly placed on such property in accordance with the provisions of this Act, he shall be liable to pay the telegraph authority such expenses (if any) as may be incurred in making good such damage, and shall also, if the telegraphic communication is by reason of the damage so caused interrupted, be punishable with a fine which may extend to Rs. 1000:

5. The telecom service providers in India have to sign a license agreement with the Department of Telecommunications for the right to provide telecom services in various parts of India. The telecom regulatory regime in India has gone through a lot of turmoil and evolution and currently any service provider wanting to provide telecom services is issued a Unified License (UL) and has to abide by the terms of the UL. Whilst most of the prohibited activities under the UL refer to specific terms under the UL itself such as non payment of fees and not fulfilling obligations under the UL, section 38 provides for certain specific prohibited activities which may be relevant for the ICT sector. These prohibited activities include:

(i) Carrying objectionable, obscene, unauthorized or any other content, messages or communications infringing copyright and intellectual property right etc., which may be prohibited by the laws of India;

(ii) Provide tracing facilities to trace nuisance, obnoxious or malicious calls, messages or communications transported through his equipment and network, to the authorised government agencies;

(iii) Ensuring that the Telecommunication infrastructure or installation thereof, carried out by it, should not become a safety or health hazard and is not in contravention of any statute, rule, regulation or public policy;

(iv) not permit any telecom service provider whose license has been revoked to use its services. Where such services are already provided, i.e. connectivity already exists, the license is required to immediately sever connectivity immediately.

(b) In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences;

1. The Department of Electronics and Information Technology (DEITY) has released the XIIth Five Year Plan on the information technology sector and the report of the Sub-Group on Cyber Security in the plan recognizes that cyber security threats emanate from a wide variety of sources and manifest themselves in disruptive activities that target individuals, businesses, national infrastructure and Governments alike.[6] The primary objectives of the plan for securing the country's cyber space are preventing cyber attacks, reducing national vulnerability to cyber attacks, and minimizing damage and recovery time from cyber attacks. The plan takes into account a number of focus areas to achieve its stated objectives, which are described briefly below:

- *Enabling Legal Framework* - Setting up think tanks in Public-Private mode to identify gaps in the existing policy and frameworks and take action to address them including addressing the privacy concerns of online users.
- *Security Policy, Compliance and Assurance* - Enhancement of IT product security assurance mechanism (Common Criteria security test/evaluation, ISO 15408 & Crypto Module Validation Program), establishing a mechanism for national cyber security index leading to national risk management framework.
- *Security Resarch&Development (R&D)* - Creation of Centres of Excellence in identified areas of advanced Cyber Security R&D and Centre for Technology Transfer to facilitate transition of R&D prototypes to production, supporting R&D projects in thrust areas.
- *Security Incident* - Early Warning and Response - Comprehensive threat assessment and attack mitigation by means of net traffic analysis and deployment of honey pots, development of vulnerability database.
- *Security awareness, skill development and training* - Launching formal security education, skill building and awareness programs.

[6] http://deity.gov.in/sites/upload_files/dit/files/Plan_Report_on_Cyber_Security.pdf

- *Collaboration* - Establishing a collaborative platform/ think-tank for cyber security policy inputs, discussion and deliberations, operationalisation of security cooperation arrangements with overseas CERTs and industry, and seeking legal cooperation of international agencies on cyber crimes and cyber security.

(c) States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

As mentioned in response to (a) above, the primary legislation in India that deals with information technology and hence ICT as well is the Information Technology Act, 2000. The IT Act contains a number of penal provisions which make it illegal to indulge in a number of practices such as hacking, online fraud, etc. which have been recognised internationally as wrongful acts using ICT (*Please refer to answer under section (a) above for details of the penal provisions*). Further section 1(2) of the IT Act provides that it also applies to any offence or contravention hereunder committed outside India by any person. This means that the IT Act also covers internationally wrongful acts using ICTs.

(d) States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect;

There are a number of ways in which states can share information by using widely accepted formal processes precisely for this purpose. Some of the most common methods of international exchange used by India are given below:

1. **MLATs**

   Although the exact process by which intelligence agencies in India share information with other agencies internationally is unclear, India is a member of Interpol and the Central Bureau of Investigation, which is a Federal/Central investigating agency functioning under the Central Government, Department of Personnel & Training and is designated as the National Central Bureau of India. A very useful tool in the effort to establish cross-border cooperation

is Mutual Legal Assistance Treaties (MLATs). MLATs are extremely important for law enforcement agencies, governments and the private sector, since they act as formal mechanisms for access to data which falls under different jurisdictions. India currently has MLATs with the following 39 countries[7]

Although MLATs are considered to be a useful mechanism to ensure international cooperation, there are certain criticisms of the MLAT mechanism, such as:

(i) The lack of clear time tables: Although MLATs do provide for broad time frames, they do not provide for more specific time tables and usually do not have any provision for an expedited process, for eg. it is believed that for requests to the U.S., processing can take from six weeks (for requests with minimal issues complying with U.S. legal standards) to 10 months.[8] Such a long time frame is clearly a burden on the investigation process and has been criticised for being ineffectual as they may not provide information fast enough;

(ii) Variation in Legal Standards: The legal standards for requesting information, for eg. the circumstances under which information can be requested or what information can be requested, differ from jurisdiction to jurisdiction. These differences are often not understood by requesting nations thus causing problems in accessing information;[9]

(ii) Inefficient Legal Process: The legal process to carry out requests through the MLAT process is often considered too cumbersome and inefficient.

(iii) Non-incorporation of technological challenges: MLATs have not been updated to meet the challenges brought about by technology, especially with the advent of networked infrastructure and ICT which raise issues of attribution and cross-jurisdictional access to information.[10]

2. Extradition

[7]List of the countries is available at http://cbi.nic.in/interpol/mlats.php
[8]https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society
[9]Peter Swire & Justin D. Hemmings, "Re-Engineering the Mutual Legal Assistance Treaty Process", http://www.heinz.cmu.edu/~acquisti/SHB2015/Swire.docx, *cf.* https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society.
[10]MLATS and International Cooperation for Law Enforcement Purposes, available at http://cis-india.org/internet-governance/blog/presentation-on-mlats.pdf

Extradition generally refers to the surrender of an alleged or convicted criminal by one State to another. More precisely, it may be defined as the process by which one State upon the request of another surrenders to the latter a person found within its jurisdiction for trial ~~and punishment~~ or, if he has been already convicted, only for punishment, on account of a crime punishable by the laws of the requesting State and committed outside the territory of the requested State. Extradition plays an important role in the international battle against crime and owes its existence to the so-called principle of territoriality of criminal law, according to which a State will not apply its penal statutes to acts committed outside its own boundaries except where the protection of special national interests is at stake. India currently has extradition treaties with 37 countries and extradition arrangements with an additional 8 countries.[11]

3. Letters Rogatory

A Letter Rogatory is a formal communication in writing sent by the Court in which an action is pending to a foreign court or Judge requesting that the testimony of a witness residing within the jurisdiction of that foreign court be formally taken under its direction and transmitted to the issuing court making the request for use in a pending legal contest or action. This request entirely depends upon the comity of courts towards each other and usages of the court of another nation.

Apart from the above methods, India also regularly signs Bilateral MoUs with various countries on law enforcement and information sharing specially in cases related to terrorism. India also regularly helps and gets helps from Interpol, the International Criminal Police Organisation for purposes of investigation, arrests and sharing of information.[12]

Other than these formal methods states sometimes share information on an informal basis, where the parties help each other purely on the basis of goodwill, or sometimes even coercion. A recent example of informal cooperation between the security agencies of India and Nepal, although not

[11]The full list of the countries with which India has agreed an MLAT is available at http://cbi.nic.in/interpol/extradition.php

[12]http://cbi.nic.in/interpol/assist.php

in the realm of cyber space, was the arrest of YasinBhatkal, leader of the banned organisation Indian Mujahideen (IM) where the Indian security agencies allegedly sought informal help from their Neapaelese counterparts to arrest a person who was wantedhad long been wanted by the Indian security agencies for a long time.[13]

In the current environment of growing ICT and increased cross-border information sharing between individuals, the role of private companies who carry this information has become much more pronounced. This changed dynamic raises new problems, especially because manyin light of thesefact that a number of these companies do not have a physical presence in all the countries where they offer services over the internet. This leads to problems for states in terms of law enforcement, speciallyespecially if they want information from these companies who do not have an incentive or desire to provide itagainst their will. These circumstances lead to a number of prickly situations where states are often frustrated in using legal and formal means and often resort to informal pressure to get the companies to agree to data localization requests, encryption/decryption standards and keys, back doors, and other requests. etc., Tthe most famous of these in the Indian context being the disagreement/ heated exchange between the Indian government and Canada based Blackberry Limited (formerly Research in Motion) for data requests on their Blackberry enterprise platform.

(e) States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;

Right to Privacy

1. The right to privacy has been recognised as a constitutionally protected fundamental right in India through judicial interpretation of the right to life which is specifically guaranteed under the Constitution of India. Since the right to privacy was read into the constitution by judicial

[13] http://www.firstpost.com/india/how-the-police-tracked-and-arrested-im-founder-yasin-bhatkal-1071755.html

pronouncements, it could be said that the right to privacy in India is a creature of the courts atleast in the Indian context. For this reason it may be useful to list out some of the major cases which deal with the right to privacy in India:

i. *Kharak Singh* v. *Union of India*,[14] (1962)

   a. For the first time, the courts recognized the right to privacy as a fundamental right, although in a minority opinion.

   b. The decision lLocated the right to privacy under both the right to personal liberty as well as freedom of movement.

ii. *Govind* v. *State of M.P.*,[15] (1975)

   a. Adopted the minority opinion of *Kharak Singh* as the opinion of the Supreme Court and held that the right to privacy is a fundamental right.

   b. An individual deDerivesd the right to privacy from both the right to life and personal liberty as well as freedom of speech and movement.

   c. The right to privacy was said to encompass and protect the personal intimacies of the home, the family marriage, motherhood, procreation and child rearing.

   d. The court established that the rRight to privacy can be violated in the following circumstances (i) important countervailing interest which is superior, (ii) compelling state interest test, and (iii) compelling public interest.

iii. *R. Rajagopal* v. *Union of India*,[16] (1994)

   a. Recognised that the rRight to privacy is a part of the right to personal liberty guaranteed under the constitution.

   b. Recognizeds that the right to privacy can be both a tort (actionable claim) as well as a fundamental right.

---

[14] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=3641

[15] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=6014

[16] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=11212

c. Established that aA citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters and nobody can publish anything regarding the same unless (i) he consents or voluntarily thrusts himself into controversy, (ii) the publication is made using material which is in public records (except for cases of rape, kidnapping and abduction), or (iii) he is a public servant and the matter relates to their discharge of official duties.

iv. *People's Union for Civil Liberties* v. *Union of India*,[17] (1996)

a. Extended the right to privacy to include communications privacy..

b. Laid down guidelines which form the backbone for checks and balances in interception provisions.

v. *District Registrar and Collector, Hyderabad and another* v. *Canara Bank and another*,[18] (2004)

a. Refers to personal liberty, freedom of expression and freedom of movement as the fundamental rights which give rise to the right to privacy.

b. The rRight to privacy deals with persons and not places.

c. Intrusion into privacy may be by - (1) legislative provisions, (2) administrative/executive orders and (3) judicial orders.

vi. *Selvi and others* v. *State of Karnataka and others*,[19] (2010)

a. The Court acknowledged the distinction between bodily/physical privacy and mental privacy

b. Subjecting a person to techniques such as narcoanalysis, polygraph examination and the Brain Electrical Activation Profile (BEAP) test without consent violates the subject's mental privacy

2. Although the judgements in the above cases (except for the case of *People's Union for Civil Liberties* v. *Union of India*) were pronounced given in a non telecomnot delivered in a

[17] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=14584

[18] http://www.judis.nic.in/supremecourt/imgs1.aspx?filename=26571

[19] http://dspace.judis.nic.in/bitstream/123456789/26592/1/36303.pdf

telecommunications context, however the ease with which these principles were applied in the case of *People's Union for Civil Liberties* v. *Union of India*, suggests that these principles, where applicable, would be applied even in the context of ICT and are not limited to only the non-digital world.

3. It must however be noted that dueDue to some incongruities in the interpretation of the earlier judgments, the Supreme Court has recently referred the matter regarding the existence and scope of the right to privacy in India to a larger bench so as to bring clarity regarding the exact scope of the right to privacy in Indian law. The very concept that the Constitution of India guarantees a right to privacy was challenged due to an "unresolved contradiction" in judicial pronouncements. This "unresolved contradiction" arose because in the cases of *M.P. Sharma & Others v. Satish Chandra & Others*,[20] and *Kharak Singh v. State of U.P. & Others*,[21](decided by*Eigh*eight*t*andsix*Six*Judges respectively) the majority judgment of the Supreme Court had categorically denied the existence of a right to privacy under the Indian Constitution.

However somehow the later case of Gobind v. *State of M.P. and another*,[22] (which was decided by a two Judge Bench of the Supreme Court) relied upon the opinion given by the minority of two judges in *Kharak Singh* to hold that a right to privacy does exist and is guaranteed as a fundamental right under the Constitution of India without addressing the fact that this was a minority opinion and that the majority opinion had denied the existeance of the right to privacy. Thereafter a large number of cases have held the right to privacy to be a fundamental right, the most important of which are *R. Rajagopal& Another* v. *State of Tamil Nadu & Others*,[23] (popularly known as *Auto Shanker's case*) and *People's Union for Civil Liberties (PUCL)* v. *Union of India & Another*.[24]

---

[20]AIR 1954 SC 300. In para 18 of the Judgment it was held: "A power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the Constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the American Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction."

[21]AIR 1963 SC 1295. In para 20 of the judgment it was held: "… Nor do we consider that Art. 21 has any relevance in the context as was sought to be suggested by learned counsel for the petitioner. As already pointed out, the right of privacy is not a guaranteed right under our Constitution and therefore the attempt to ascertain the movement of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III."

[22](1975) 2 SCC 148.

[23](1994) 6 SCC 632.

[24](1997) 1 SCC 301.

However, as was noticed by the Supreme Court in its August 11, 2015 order, all these judgments were decided by two or three Judges only which could not have overturned the judgments given by larger benches.[25] It was to resolve this judicial incongruity that the Supreme Court referred this issue to a larger bench to decide on the existence and scope of the right to privacy in India.

Freedom of Expression

4. Freedom of expression is one of the most important fundamental rights guaranteed under the constitution and has been vehemently protected by the judiciary on a number of occasions whenever it has been threatened. With the advent of social media, the entire dynamics of the freedom of speech and expression have changed in that it is now possible for every individual, with an internet connection and a Ffacebook/Ttwitter/Wwhatsapp account to reach millions of people without spending any extra money. This ability to reach a much larger and wider audience also led to greater friction between people holding different opinions. As the ease of the internet removed the otherwise filtering effects of geography and made it easier for people to communicate with each other, the advent of social media made it easier for them to communicate with a larger number of people at the same time. This ability to communicate within a group also gave rise to "debates" which often turngot ugly, highlighting giving way to concerns of how easy it is to harrass people on social media.

5. This concernConcern over of harassment led a number of people to call for greater censorship of social media and it was perhaps this concern which gave rise to the biggest challenge to the freedom of speech and expression in the online world, in the form of section 66A of the Information Technology Act, 2000 which made it an offense to send information which was "grossly offensive" (s.66A(a)) or caused "annoyance" or "inconvenience" while being known to be false (s.66A(c)). This section was used widely seen by Oonline activists, including the Centre for Internet and Society, widely considered this section as a tool for the government to silence those who criticised it. Infact, statistics compiled by the National Crime Records Bureau from 2014 revealed that 2,402

[25] http://cis-india.org/internet-governance/blog/right-to-privacy-in-peril

people, including 29 women, were arrested in 4,192 cases under section 66A which accounted for nearly 60% of all arrests under the IT Act, and 40% of arrests for cyber crimes in 2014.[26]

6. The section was finally struck down by the Supreme Court in 2015 in the case of *Shreya Singhal*v. *Union of India*,[27] on the ground of being too vague. This decision was seen as a huge victory for the campaign for freedom of speech and expression in the virtual world since this section was frequently used by the state (or rather government in power) to muzzle free speech against the incumbent government or political leaders. The offending section 66A made it an offence to send any information that was "grossly offensive or has menacing character" or "which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, or ill will, persistently makes by makinguse of such computer resource or a communication device,". These terms quoted above were held by the Court to be too vague and wide and falling foul of the limited restrictions constitutionally imposed on the freedom of expression. The Supreme Court therefore , and were therefore struck down section 66A by the Supreme Court.

(f) A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public;

The researchers of this report could not locate any norms in India which address this issue. To the best of their knowledge, India does not support any ICT activity that intentionally damages critical infrastructure or impairs the use and operation of critical infrastructure.

(g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions;

[26] http://cis-india.org/internet-governance/news/hindustan-times-august-20-2015-aloke-tikku-stats-from-2014-reveal-horror-of-scrapped-section-66-a-of-it-act

[27] http://supremecourtofindia.nic.in/FileServer/2015-03-24_1427183283.pdf

1. Section 70 of the IT Act gives the government the authority to declare any computer system which directly affects any critical information infrastructure to be a protected system. The term "critical information infrastructure" (CII) is defined in the IT Act "the computer resource, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety." Once the government declares any computer resource as a protected system it gets the authority to prescribe information security practices for such as system as well as identify the persons who are authorised to access such systems. Any person who accesses a protected system in contravention of the provision of Section 70 of the IT Act shall be liable to be imprisoned for a maximum period of 10 years and also pay a fine. Further, section 70A of the IT Act gives the government the power to name a national nodal agency in respect of CII and also prescribe the manner for such agency to perform its duties. In pursuance of the powers under sections 70A the government has designated the National Critical Information Infrastructure Protection Centre (NCIIPC) situated in the JNU campus as the nodal agency.[28] This agency is a part of and under the administrative control of the National Technical Research Organisation (NTRO).[29]

2. The functions and manner of performing such functions by the NCIIPC has been prescribed in the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.[30] According to these Rules the functions of the NCIIPC include, inter alia, (i) the protecting and giving advice to reduce the vulnerabilities of CII against cyber terrorism, cyber warfare and other threats; (ii) identification of all critical infrastructure elements so that they can be notified by the government; (iii) providing strategic leadership and coherence across the government to respond to cyber security threats against CII; (iv) coordinating, sharing, monitoring, analysing and forecasting national level threats to CII for policy guidance, expertiese sharing and situational awareness for early warning alerts; (v) assisting in the development of appropriate plans, adoption of standards, sharing best practices and refinining procurement processes for CII; (vi) undertaking and funding research and development to innovate future technologies and collaborate with PSUs, academia and international partners for

[28] http://deity.gov.in/sites/upload_files/dit/files/S_O_18(E).pdf

[29]

[30] http://deity.gov.in/sites/upload_files/dit/files/GSR_19(E).pdf

protection of CII; (vii) organising training and awareness programmes and development of audit and certification agencies for protection of CII; (viii) developing and executing national and international cooperation strategies for protection of CII; (ix) issuing guidelines, advisories and vulnerability notes relating to CII and practices, procedures, prevention and responses in consultation with CERT-In and other organisations; (x) exchanging information with CERT-In, especially in relation to cyber incidents; and (xi) calling for information and giving directions to critical sectors or persons having a critical impact on CII, in the event of any threat to CII.[31]

3. The NCIIPC had in the year 2013 released (non publicly) Guidelines for the Protection of National Critical Information Infrastructure[32] (CII Guidelines) which presented 40forty controls and respective guiding principles for the protection of CII. It is expected that these controls and guiding principles will help critical sectors to draw a CII protection roadmap to achieve safe, secure and resilient CII for India. The 'Guidelines for forty Critical Controls' is considered by the NCIIPC to be a significant milestone in its efforts for the protection of nation's critical information assets. These fort controls can be found in Section 6 (Best Practices, Controls and Guidelines) of the CII Guidelines. It must be noted that the CII Guidelines were drafted after taking inputs from a number of stakeholders such as the national Stock Exchange, the Airports Authority of India, National Thermal Power Corporation, Reserve Bank of India, Indian Railways, Telecom Regulatory Authority of India, Bharat Sanchar Nigam Limited, etc. This exercise of taking inputs from different stakeholders as well as developing a standard of as many as 40forty aspects of security seems to suggest that the NCIIPC is taking steps in the right direction.

4. The Recommendations on Telecommunication Infrastructure Policy issued by the Telecom Regulatory Authority of India in April, 2011 are silent on the issue of security of critical information infrastructure.s. However, the National Policy on Information Technology, 2012 (NPIT) does address the issue of security of cyber space by saying that the government should make efforts to do the following:

---

[31]Rule 4 of the Information Technology (National Critical Information Infrastructure Protection Centre and Manner of Performing Functions and Duties) Rules, 2013.

[32]Since these Guidelines were not publicly released they are not available on any government website. In this paper we have relied on a version available on a private website at http://perry4law.org/cecsrdi/wp-content/uploads/2013/12/Guidelines-For-Protection-Of-National-Critical-Information-Infrastructure.pdf

"9.1 To undertake policy, promotion and enabling actions for compliance to international security best practices and conformity assessment (product, process, technology & people) and incentives for compliance.

9.2 To promote indigenous development of suitable security techniques & technology through frontier technology research, solution oriented research, proof of concept, pilot development etc. and deployment of secure IT products/processes

9.3 To create a culture of cyber security for responsible user behavior & actions including building capacities and awareness campaigns.

9.4 To create, establish and operate an 'Information Security Assurance Framework'."

5. The Department of Information and Technology has formed the Computer Emergency Response Term of India (CERT-In) to enhance the security of India's Communications and Information Infrastructure through proactive action and effective collaboration. The Information Security Policy on Protection of Critical Infrastructure released by the CERT-In considers information recorded, processed or stored in electronic medium as a valuable asset and is geared towards protection of such "valuable asset". The policy recognises the importance of critical information infrastructure network and says that any disruption of the operation of such networks is likely to have devastating effects. The policy prescribes that personnel with program delivery responsibilities should also recognise the importance of security of information resources and their management. Thus Ddue to this recognition of the growing networked nature of government as well as critical organisations and the need to have a proper vulnerability analysis as well as effective management of information security risks, the Department of Technology prescribes the following information security policy:

"In order to reduce the risk of cyber attacks and improve upon the security posture of critical information infrastructure, Government and critical sector organizations are required to do the following on priority:

- Identify a member of senior management, as Chief Information Security Officer (CISO), knowledgeable in the nature of information security & related issues and designate him/her as a 'Point of contact', responsible for coordinating security policy compliance efforts and to regularly interact with the Indian Computer Emergency Response Team (CERT-In), Department of

Information Technology (DIT), which is the nodal agency for coordinating all actions pertaining to cyber security;

- Prepare information security plan and implement the security control measures as per ISI/ISO/IEC 27001: 2005 and other guidelines/standards, as appropriate;
- Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/ functions and achievement of organisational goals/objectives;
- Periodically test and evaluate the adequacy and effectiveness of technical security control measures implemented for IT systems and networks. Especially, Test and evaluation may become necessary after each significant change to the IT applications/systems/networks and can include, as appropriate the following:
    - ➢ Penetration Testing (both announced as well as unannounced)
    - ➢ Vulnerability Assessment
    - ➢ Application Security Testing
    - ➢ Web Security Testing
- Carry out Audit of Information infrastructure on an annual basis and when there is major upgradation/change in the Information Technology Infrastructure, by an independent IT Security Auditing organization;

    .....

- Report to CERT-In the cyber security incidents, as and when they occur and the status of cyber security, periodically."

6. The Department of Electronics and Information Technology (DEITY) released the National Policy on Electronics in 2012 which contained the government's take on the electronics industry in India. Section 5 of the said policy talks about cCyber sSecurity and states that to create a complete secure cyber eco-system in the country, careful and due attention is required for creation of well-d defined technology and systems, use of appropriate technology and more importantly development of appropriate products and& solutions. The priorities for action should be suitable design and development of indigenous appropriate products through frontier technology/product

oriented research, testing and& validation of security of products meeting the protection profile requirements needed to secure the ICT infrastructure and cyber space of the country.

7. In addition the CERT-In has issued an Information Security Management Implementation Guide for Government Organisations.[33] CERT-In has also prescribed progressive steps for implementation of Information Security Management System in Government & Critical Sectors as per ISO 27001. The steps prescribed are as follows:

- Identification of a Point-of-Contact (POC) / Chief Information Security Officer (CISO) for coordinating information security policy implementation efforts and communication with CERT-In
- Information Security Awareness Programme
- Determination of general Risk environment of the organization (low / medium / hHigh) depending on the nature of web and& networking environment, criticality of business functions and impact of information security incidents on the organization, business activities, assets / resources and individuals
- Status appraisal and gap analysis against ISO 27001 based best information security practices
- Risk assessment covering evaluation of threat perception and technical and &operational vulnerabilities
- Comprehensive risk mitigation plan including selection of appropriate information security controls as per ISO 27001 based best information security practices
- Documentation of agreed information security control measures in the form of information security policy manual, procedure manual and work instructions
- Implementation of information security control measures (Managerial, Technical and& operational)
- Testing & evaluation of technical information security control measures for their adequacy & effectiveness and audit of IT applications/systems/networks by an independent

[33]Available at http://www.cert-in.org.in/

information security auditing organization (penetration testing, vulnerability assessment, application security testing, web security testing, LAN audits, etc)

- Information Security Management assessment and certification against ISO 27001 standard, preferably by an independent & accredited organization

8. The Unified License for providing various telecommunication services also discusses contains certain terms which talk about how to engagedeal with telecommunication infrastructure in light of national security, which include the following recommendations:

- providing necessary facilities to the Government to counteract espionage, subversive act, sabotage or any other unlawful activity;
- giving full access to its network and equipment to the authorised persons for technical scrutiny and inspection;
- obtaininggettting security clearance for all foreign nationals deployed on for installation, operation and maintenance of the network;
- being completely responsible for the security of its network and having organizational policy on security and security management of its network including Network forensics, Network Hardening, Network penetration test, Risk assessment;
- auditing its network or getting the network audited from security point of view once in a financial year from a network audit and certification agency;
- inducting only those network elements into its telecommunications network, which have been got tested according tos per relevant contemporary Indian or International Security Standards;
- including all contemporary security related features (including communication security) as prescribed under relevant security standards while procuring the equipment and implementing all such contemporary features into the network;
- keeping requisite records of operations in the network;
- monitoring of all intrusions, attacks and frauds on his technical facilities and provide reports on the same to the Licensor.

Further statutory restrictions on tampering critical infrastructure are already contained in the Telegraph Act and have been discussed above, though the penalties provided may need to be increased if they are to act as a deterrent in this age where the stakes are much higher.

(h) States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty;

There is yet to be a publicly acknowledged request from a foreign government asking the Indian government to take steps to prevent malicious ICT acts originating from its territory.

(i) States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions;

Section 4 of the National Electronics Policy, 2012 talks about "Developing and Mandating Standards" and says that in order to curb the inflow of sub-standard and unsafe electronic products the government should mandate technical and safety standards which conform to international standards and do the following:

a.Ddevelop Indian standards to meet specific Indian conditions including climatic, power supply,, and handling and other conditions etc., by suitably reviewing existing standards.

b. Mmandate technical standards in the interest of public health and safety

c. Sset up an institutional mechanism within Department of Information Technology for mandating compliance to standards for electronics products.

d. Ddevelop a National Policy Framework for enforcement and use of Standards and Quality Management Processes.

e.Sstrengthen the lab infrastructure for testing of electronic products and encouraging development of conformity assessment infrastructure by private participation.

f. Ccreate awareness amongst consumers against sub-standard and spurious electronic products.

g. Bbuild capacity within the Government and public sector for developing and mandating standards.

h. Aactively participate in the international development of standards in the Electronic System Design and Manufacturing sector.

(j) States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;

Under section 70B of the IT Act, India has established a Computer Emergency Response Team (CERT-In) to serve as the national agency for incident responses. The functions mandated to be performed by CERT-In as per the IT Act are:

(a) Ccollection, analysis and dissemination of information on cyber incidents;

(b) Fforecasting and alerts of cyber security incidents;

(c) Eemergency measures for handling cyber security incidents;

(d) Coordination of cyber incidents response activities;

(e) Iissuing ofe guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response and reporting of cyber incidents;

(f) Ssuch other functions relating to cyber security as may be prescribed.

CERT-In also publishes information regarding various cyber threats on its websites so as to keep internet users aware of the latest threats in the online world. Such information can be accessed both on the main page of the CERT-In website or under the Advisories section on the website.[34]

[34] http://www.cert-in.org.in/

(k) States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cyber security incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

There are no official or public reports of India using its CERT-In to harm the information systems of another state, although it is highly unlikely that any state would publicly acknowledge such activities even if it was indulging in them.

CONCLUSION

The As can be seen from the discussion above, the statutory, regulatory and policy regime in India does seem to address most of thcyber securitye norms in some manner or the other, but these efforts almostalmost always fall short of meeting some of the norms. While the Information Technology Act along with the Rules thereunder, as being the umbrella legislation for digital transactions in India, does address some of the issues mentioned above, it does not address some of the problems that arise out of a greater reliance on the internet such as spamming, trolling, and, online harassment, etc. Although some of these acts may be addressed by regular legislation by applying them in the online world however this does not always take into account the unique features and complexities of committing these acts/crimes in the online world.

In the area of exchange of information between states, India has entered into a number of MLATs and eExtradition treaties, and frequently issues Letters of Rogatory. Yet however these mechanisms may not be adequate to address the needs of crime prevention of crimes in the age of ICT, as crime preventionit often requires exchange of information inon r a real time basis which is not possible with the bureaucratic procedures involved in the MLAT process. There also needsd to be stronger standards which are applicable to ICT equipment, including imported equipment especially in light of the fact that security concerns related to Chinese ICT equipment that from China have been raised quite frequently in the past. There also needs to be a better system of reporting ICT vulnerabilities to CERT-In or other authorized agencies so that mitigation measure can be implemented in time.

It should be noted that the work of the Group of Experts is not complete since the General Assembly has asked the Secretary General to form a new Group of Experts which would report back to the Secretary General in 2017. It is imperative that the Government of India realise the importance of the work being done by the Group of Experts and take measures to ensure that a representative from India is included in or atleast the comments and concerns of India are included and addressed by the Group of Experts. Meanwhile, India can begin by strengthening domestic privacy safeguards, improving transparency and efficiency of relevant policies and processes, and looking towards solutions that respect rights and strengthen security. Brutent force solutions such

as demands for back doors, unfair and unreasonable encryption regulation, and data localization requirements will not help propel India forward in international discussions, dialogues, or agreements on cross-border sharing of information. Though the recommendations from the Group of Experts are welcome, beyond a preliminary mention of privacy and freedom of expression, the rights of individuals – and the ways in which these can be protected, various components that go into supporting those rights including redress, transparency, and due process measures - was inadequately addressed.