Remark: This is a draft structure Bill based on stakeholder consultations and international best practices. The drafter tried to base the legal drafting style on customs used in other pieces of legislation enacted in Nepal such as the Electronic Transactions Act. However, it requires adjustments to fully customize it to national practice and ensure that conflicts with other existing legislation are avoided.

Draft version: 0.8 (not yet finalized)

The Cybercrime Act, xx (2018)

Date of Authentication and Publication

Act number xx of the year 2018

And Act promulgated for Cybercrime

Preamble:

WHEREAS, it is essential to underline the relevance that information and communication technology has for the citizens of Nepal,
And whereas a foundation to foster the development was laid out by the National Broadband Policy, the National ICT Policy and the National Cybersecurity Policy,
And whereas it is expedient to develop an updated legal framework that safeguard the security of electronic systems and networks by criminalizing serious violations,
Now, therefore, be it enacted by the House of Representatives in the xx Year of the issuance of the Proclamation of the House of Representatives, 2063(2007).

Chapter – 1

Preliminary

1. **Short Title, Extension and Commencement: (**1) This Act may be called "The Cybercrime Act, x (2018)".

(2) This Act shall be deemed to have been commenced from

(3) This Act shall extend throughout Nepal and shall also apply to any person residing anywhere by committing an offence in contravention to this Act.

2. **Definitions:** Unless the subject or context otherwise requires, in this Act,-

a) "Access" means means an opportunity of gaining entry into, logical, arithmetical or resources of memory function of any electronic system, computer system or network;

b) "Access provider" means any person providing any electronic communication transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network;

c) "Caching provider" means any person providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request;

d) "Child" means a minor not having completed the age of sixteen years;

e) "Child pornography" means material that, -

   i. depicts or presents a child engaged in sexually explicit conduct; or

   ii. depicts or presents a person appearing to be a child engaged in sexually explicit conduct; or

   iii. realistically represents a person appearing to be child engaged in sexually explicit conduct;

this includes, but is not limited to, any visual (images, animations or videos), audio or text material.

f) "Critical infrastructure" means electronic systems, devices, networks, computer programs, electronic data, vital for

   i. the security, defense or international relations of Nepal ; or

   ii. the existence or identity of a confidential source of information relating to the enforcement of criminal law; or

   iii. the provision of services directly related to communications infrastructure, banking and financial services, public utilities, courts, public transportation, public key infrastructure, payment systems infrastructure or e-commerce infrastructure; or

   iv. the protection of public safety including systems related to essential emergency services such as police, civil defense and medical services;

   v. the purpose declared as such by the Ministry of Defense in accordance with the prescribed procedure;

where the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on the country.

g) “Electronic” includes but not limited to electrical, digital, analogue, magnetic, optical, biochemical, electrochemical, electromechanical, electromagnetic, radio electric or wireless technology;

h) “Electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by electronic means;

i) “Electronic data” means any representation of facts, concepts, information (being either texts, images, audio, or video) machine-readable code or instructions, in a form suitable for processing in an electronic system, including a program suitable to cause an electronic system to perform a function;

j) “Electronic device” means any hardware or equipment which performs one or more specific functions and operates on any form or combination of electrical energy and includes but is not limited to

   i. components of electronic systems such as computer, graphic cards, mobile phones, memory, chips;
   ii. storage components such as hard drives, memory cards, compact discs, tapes;
   iii. input devices such as keyboards, mouse, track pad, scanner, digital cameras;
   iv. output devices such as printer, screens;

k) “Electronic mail message” means any data generated by an electronic system for one or more electronic mail addresses;

l) “Electronic storage medium” means any article or material (for example, a disk) from which information is capable of being reproduced, with or without the aid of any other article or device.

m) “Electronic system” means any electronic device or a group of interconnected or related devices, one or more of which, pursuant to a program or manual or any external instruction, performs automatic processing of information or electronic data and may also include a permanent, removable or any other electronic storage medium;

n) “Hinder” in relation to an electronic system includes but is not limited to:

   i. cutting the electricity supply to an electronic system; or
   ii. causing electromagnetic interference to an electronic system; or
   iii. corrupting an electronic system by any means; or
   iv. damaging, deleting, deteriorating, altering or suppressing electronic data;

o) “Hosting provider” means any person providing an electronic data transmission service by storing of information provided by a user of the service;

p) “Information” includes text, message, data, voice, sound, database, video, signals, software, computer programs, codes including object code and source code;

q) “Interception” means tapping into an electronic communication not directed to the one who is tapping in including but is not limited to the acquiring, viewing and capturing of any electronic communication whether by wire, wireless, electronic, optical, magnetic, or other means, during transmission through the use of any technical device;

r) “Internet Service Provider” means a natural or legal person that provides to users services mentioned in Sections 27-29;

s) “Remote Forensic Tool” means an investigative tool such as software or hardware installed on or applied with regard to an electronic system and used to perform tasks that include but are not limited to keystroke logging or transmission of an IP-address;

t) “Seize” includes:

   i. activating any onsite electronic system and electronic storage media;
   ii. making and retaining a copy of electronic data, including by using onsite equipment;
   iii. maintaining the integrity of the relevant stored electronic data;
   iv. rendering inaccessible, or removing, electronic data in the accessed electronic system;
   v. taking a printout of output of electronic data; or
   vi. secure an electronic system or part of it or an electronic storage medium;

u) “Spam” means the unsolicited transmission of a harmful, fraudulent, misleading or illegal electronic mail message to any person or causing an electronic system to show such message for commercial or illegal purpose.

v) “Traffic data” means electronic data that:

   1) relates to a communication by means of an electronic system; and
   2) is generated by an electronic system that is part of the chain of communication ; and
   3) shows the communication’s origin, destination, route, time date, size, duration or the type of underlying services;

w) “Thing” includes but not limited to:

   1) an electronic system or part of an electronic system;
   2) another electronic system, if:
      i. electronic data from that electronic system is available to the first electronic system being searched; and
      ii. there are reasonable grounds for believing that the electronic data sought is stored in the other electronic system;
   3) an electronic data storage medium.

Chapter – 2

Jurisdiction

3. Jurisdiction

Notwithstanding anything contained in the prevailing laws, if any person commits any act or an omission which constitutes an offence under this Act

i. in the territory of Nepal; or

ii. on a ship or aircraft registered in Nepal; or

iii. by a national of Nepal outside the territory of Nepal if the person's conduct would also constitute an offence under a law of the country where the offence was committed; or

iv. by a national of Nepal outside the jurisdiction of any country

a case may be filed against such a person and shall be punished accordingly.

Chapter – 3

Offences Related to Electronic Systems and Electronic Data

4. Illegal Access to an Electronic System

1) If any person wilfully and with mala fide intention, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of an electronic system by infringing security measures, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both.
2) If the act described in Subsection (1) includes wilful and mala fide access to critical infrastructure the person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both.

Explanation: (to be deleted in the final version): In the following provisions "wilfully" will mainly be used to describe the *mens rea*. The provision above includes wilful and with mala fide as international and regional models (such as the Council of Europe Convention on Cybercrime) allow such restriction with regard to illegal access. With regard to most other provisions such restriction is not allowed. In order to meet those standards the restriction was not included in other provisions.

5. Illegal Remaining in am Electronic System

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in an electronic system or part of an electronic system or continues to use an electronic system, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

.

6. Illegal Interception

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means:

i. any non-public transmission to, from or within an electronic system; or
ii. electromagnetic emissions from an electronic system

such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

7. Illegal Data Interference

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, interferes with an electronic data owned or managed by someone else by doing any of the following acts:

i. damages or deteriorates electronic data; or
ii. deletes electronic data; or
iii. alters electronic data; or
iv. renders electronic data meaningless, useless or ineffective; or
v. obstructs, interrupts or interferes with the lawful use of electronic data; or
vi. obstructs, interrupts or interferes with any person in the lawful use of electronic data; or
vii. denies access to electronic data to any person authorized to access it;

such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

8. Illegal Acquisition of Data

1) If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, obtains, for himself or for another, electronic data which are not meant for him, and which are not public or protected against unauthorized access, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.
2) If the act described in Subsection (1) includes confidential electronic data such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

9. Illegal System Interference

1) If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification:
   i. Hinders, denies or interferes with the functioning of an electronic system; or
   ii. Hinders, denies or interferes with a person who is lawfully using or operating an electronic system;

   such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both.
2) If the act described in Subsection (1) affects an electronic system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

10. Illegal Devices

1) If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:

i. a software, electronic system or an electronic device, that is designed or adapted for the purpose of committing an offence defined by Section 4-9 of this Act and that is contained in a schedule published by Nepal Telecommunications Authority; or

ii. a password, access code or similar data by which the whole or any part of an electronic system or electronic data is capable of being accessed;

with the intent that it be used by any person for the purpose of committing an offence defined by Section 4-9 of this Act, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

2) If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification has an item mentioned in Subparagraph (1) (i) or (1) (ii) in possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Section 4-9 of this Act, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

3) Explanation: This provision 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 Subsection 1 is not for the purpose of committing an offence established in accordance with other provisions of Section 4-9 of this Act, such as for the authorized testing or protection of an electronic system.

11. <u>Electronic Forgery</u>

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses electronic 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, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

12. <u>Electronic Fraud</u>

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, causes a loss of property to another person by:

i. any input, alteration, deletion or suppression of electronic data;

ii. any interference with the functioning of an electronic system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person, such a person shall be liable to the punishment with the fine not

exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

13. Child Pornography

1) If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification
   i. produces child pornography for the purpose of its distribution through an electronic system;
   ii. offers or makes available child pornography through an electronic system;
   iii. distributes or transmits child pornography through an electronic system;
   iv. procures and or obtains child pornography through an electronic system for oneself or for another person;
   v. possesses child pornography in an electronic system or on an electronic storage medium; and
   vi. knowingly obtains access, through electronic system, to child pornography,

such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

2) **Explanation:** It is a defense to a charge of an offence under Subsection (1) (ii) to Subsection (1) (vi) if the person establishes that the child pornography was offered, distributed, procured or kept for bona fide religious, research, law enforcement or medical purposes. If child pornography was stored for such purpose, the authorized persons need to ensure that it is deleted as soon as it is not legally required anymore.

14. Pornography

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification by using an electronic system in any stage of the offence, makes pornography available to one or more children or facilitates the access of children to pornography such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

15. Identity-Related Crime

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification by using an electronic system in any stage of the offence, transfers, possesses, or uses a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

16. Solicitation of Children

If any person wilfully, through an electronic system proposes to a child, to meet him or her, with the intent of sexually exploiting the child, whether or not such proposal has been followed by material acts, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

Chapter – 4

Investigations and Evidence

17. Admissibility of Electronic Evidence

In proceedings for an offence against a law of Nepal, the fact that evidence has been generated from an electronic system does not by itself prevent that evidence from being admissible.

18. Search and Seizure

1) If the [court /Information Technology Tribunal], based on an application by a police officer and on the basis of [sworn evidence] [affidavit][reasonable information] is satisfied, that there are reasonable grounds [that there may be in a place an electronic device or electronic data:
    i. that may be material as evidence in proving an offence; or
    ii. that has been acquired by a person as a result of an offence;

   the [court/Information Technology Tribunal] may issue a warrant authorizing a police officer, with such assistance as may be necessary, to enter the place to search and seize the electronic device or electronic data including search or similar access:

a) an electronic system or part of it and electronic data stored therein; and
b) an electronic storage medium in which electronic data may be stored in the territory of Nepal.

2) Any person who makes a search or seizure under this section, shall at the time or as soon as practicable:
    i. make a list of what has been seized, with the date and time of seizure; and
    ii. give a copy of that list to [xxx]
    iii. the occupier of the premises; or
    iv. the person in control of such electronic devices.
3) Subject to Subsection (4), on request, police officer or another authorized person shall:
    i. permit a person who had the custody or control of the electronic devices, or someone acting on their behalf to access and copy electronic data on the system; or
    ii. give the person a copy of the electronic data.
4) The police officer or another authorized person may refuse to give access or provide copies if he or she has reasonable grounds for believing that giving the access, or providing the copies may —
    i. constitute a criminal offence; or
    ii. prejudice
        1. the investigation in connection with which the search was carried out;
        2. another ongoing investigation; or
        3. any criminal proceedings that are pending or that may be brought in relation to any of those investigations.
5) If police officer that is undertaking a search based on Subsection (1) has grounds to believe that the data sought is stored in another electronic system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he or she shall be able to expeditiously extend the search or similar access to the other system.
6) Police officer that is undertaking a search is empowered to seize or similarly secure electronic data accessed according Subsection (1) and Subsection (2).

19. <u>Assistance</u>

A person who is not a suspect of a crime but is in possession or control of an electronic device or electronic data that is the subject of a search under Section 18 (1) shall at his own cost permit, and assist if required, the police officer making the search to —

i. access and use an electronic device or electronic data;

ii. obtain and copy that electronic data;
iii. use an electronic device to make copies; and
iv. obtain an intelligible output from an electronic device in a format that can be read.

20. <u>Production Order</u>

If the [court/Information Technology Tribunal] on application by a police officer is satisfied on the basis of [sworn evidence] [affidavit][reasonable information] that specified electronic data or a printout or other information is reasonably required for the purpose of a criminal investigation or criminal proceedings, it may order:

i. a person in control of an electronic device or electronic system of electronic devices to produce specified electronic data or printout of such information; and
ii. a service provider to produce information about persons who subscribe to or use their services.

21. <u>Expedited Preservation</u>

1) If a police officer not below the rank of the sub-inspector is satisfied that:
   i. electronic data stored in an electronic device is reasonably required for the purpose of a criminal investigation; and
   ii. there is a risk that the data may be destroyed or rendered inaccessible;

   the police officer may, by written notice given to a person in control of the electronic device, require the person to ensure that the data specified in the notice be preserved for a period of up to 7 days as specified in the notice.
2) The [court/Information Technology Tribunal] may upon application authorize an extension not exceeding 14 days.

22. <u>Partial Disclosure</u>

1) If the [court/Information Technology Tribunal] on application by a police officer is satisfied on the basis of [sworn evidence] [affidavit][reasonable information] that specified data stored in an electronic device or system of electronic devices is required for the purpose of a criminal investigation or criminal proceedings, the [court/Information Technology Tribunal] may order such person to disclose sufficient traffic data about a specified communication to identify:
   i. the service providers; and
   ii. the path through which the communication was transmitted.

2) In investigations where based on reasonable information an immediate threat to the life of a victim exists, a police officer not below the rank of the sub-inspector, that is satisfied that specified data stored in an electronic device or system of electronic devices is required for the purpose of saving the life of the victim may order such person to disclose sufficient traffic data about a specified communication to identify:
    i. the service providers; and
    ii. the path through which the communication was transmitted.

23. <u>Collection of Traffic Data</u>

1) If the [court/Information Technology Tribunal] on application by a police officer is satisfied on the basis of [sworn evidence] [affidavit][reasonable information] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [court/Information Technology Tribunal] may, by written notice given to a person in control of such data, request that person to:
    i. collect or record traffic data associated with a specified communication during a specified period in real time; and
    ii. permit and assist police officer to collect or record that data in real time.
2) If the [court/Information Technology Tribunal] on application by a police officer is satisfied on the basis of [sworn evidence] [affidavit][reasonable information] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [court/Information Technology Tribunal] may authorize any police officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means n real time.

24. <u>Lawful Interception of Content Data</u>

If the [court/Information Technology Tribunal] on application by a police officer is satisfied on the basis of [sworn evidence] [affidavit][reasonable information] that content of electronic communications is reasonably required for the purposes of a criminal investigation, the [court/Information Technology Tribunal] may:

i. order a service provider whose service is available in Nepal through application of technical means to collect or record, to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of an electronic system in real time; or

ii. authorize a police officer to collect or record that data through application of technical means in real time.

25. Forensic Tools

1) If the [court/Information Technology Tribunal] on application by a police officer is satisfied on the basis of [sworn evidence] [affidavit][reasonable information] that in an investigation concerning an offence listed in Subsection (7) herein below there are reasonable grounds to believe that essential evidence can not be collected by applying other instruments listed in Chapter 4 but is reasonably required for the purposes of a criminal investigation, the [court/Information Technology Tribunal] may authorize a police officer to utilize a remote forensic tool with the specific task required for the investigation and install it on the suspect's or his service provider's electronic system in order to collect the relevant evidence. The application needs to contain the following information:
    i. suspect of the offence and his service provider, if possible with name and address, and
    ii. description of the targeted electronic system, and
    iii. description of the intended measure, extent and duration of the utilization, and
    iv. reasons for the necessity of the utilization.
2) Within such investigation it is necessary to ensure that modifications to the electronic system of the suspect or his service provider are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation it is necessary to log:
    i. the technical mean used and time and date of the application; and
    ii. the identification of the electronic system and details of the modifications undertaken within the investigation; and
    iii. any information obtained.

   Any such information obtained by the use of such software need to be protected against any modification, unauthorized deletion and unauthorized access.
3) The duration of authorization in Subsection (1) is limited to 3 months. If the conditions of the authorization are no longer met, the action taken are to stop immediately.
4) If the installation process requires physical access to a place the requirements of Section 18 need to be fulfilled.
5) If necessary police officer may pursuant to the order granted in Subsection (1) above requests that the [court/Information Technology Tribunal] order a service provider to support the installation process.

6) [List of offences]

Chapter – 5

Criminal Liability of Internet Service Provider

26. No Monitoring Obligation

Internet service providers do not have a general obligation to monitor the information which they transmit or store on behalf of another, nor do they have a general obligation to actively seek facts or circumstances indicating illegal activity to avoid criminal liability. This provision does not affect the possibility for a court to require an Internet service provider to terminate or prevent an infringement based on any law enacted in Nepal.

27. Access Provider

1) An Access provider is not criminally liable for providing access and transmitting information on condition that the provider:
   i. does not initiate the transmission;
   ii. does not select the receiver of the transmission; or
   iii. does not select or modify the information contained in the transmission.
2) The acts of transmission and of provision of access referred to in paragraph 1 include the automatic, intermediate and transient storage of the information transmitted in so far as this takes place for the sole purpose of carrying out the transmission in the communication network, and provided that the information is not stored for any period longer than is reasonably necessary for the transmission.

28. Hosting Provider

1) A Hosting provider is not criminally liable for the information stored at the request of a user of the service, on condition that:
   i. the Hosting provider expeditiously removes or disables access to the information after receiving an order from any public authority or court of law to remove specific illegal information stored; or
   ii. the Hosting provider, upon obtaining knowledge or awareness about specific illegal information stored by other ways than an order from a public authority,

expeditiously takes appropriate action to remedy and inform [the relevant public authority] to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.

2) Subparagraph (1) shall not apply when the user of the service is acting under the authority or the control of the Hosting provider.

3) If the Hosting provider is removing the content pursuant to Subparagraph (1) he is exempted from contractual obligations with his customer to ensure the availability of the service.

29. <u>Caching Provider</u>

A Caching provider is not criminally liable for the automatic, intermediate and temporary storage of that information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their request, on condition that:

i. the Caching provider does not modify the information;

ii. the [Caching provider] complies with conditions of access to the information;

iii. the Caching provider complies with rules regarding the updating of the information, specified in a manner widely recognised and used by industry;

iv. the Caching provider does not interfere with the lawful use of technology, widely recognised and used by industry, to obtain data on the use of the information; and

v. the Caching provider acts expeditiously to remove or to disable access to the information it has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

Chapter – 6

Miscellaneous

30. Government of Nepal may issue Directives:

Government of Nepal may, in regard to the implementation of this Act, issue necessary directives to Telecommunication and Internet Service Providers and in such a case, it shall be a duty of the Internet Service Providers, as the case may be, to comply with such directives.

31. Power of Frame Rules:

Government of Nepal may in order to fulfill the objective of this Act, frame necessary Rules.

32. To Frame and Enforce the Directive:

To Frame and Enforce the Directives: Government of Nepal may, in order to achieve the objective of this Act, frame and enforce necessary directives, subject to this Act and Rules framed hereunder.

Appendix 1

Sample Language for Provisions Discussed during Stakeholder Consultations

A. Pornography (different approach – not limited to interaction with children)

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification

i. produces pornography for the purpose of its distribution through an electronic system;
ii. offers or makes available pornography through an electronic system;
iii. distributes or transmits pornography through an electronic system;
iv. procures and or obtains pornography through an electronic system for oneself or for another person;
v. possesses pornography in an electronic system or on an electronic storage medium; and
vi. knowingly obtains access, through electronic system, to pornography,

such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

C. Racist and Xenophobic Material

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification

i. produces racist and xenophobic material for the purpose of its distribution through an electronic system;
ii. offers or makes available racist and xenophobic material through an electronic system;
iii. distributes or transmits racist and xenophobic material through an electronic system;

such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

D. **Racist and Xenophobic Insult**

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, through an electronic system

i. persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or
ii. a group of persons which is distinguished by any of these characteristics

such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

E. **Denial of Genocide and Crimes against Humanity**

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, distributes or otherwise makes available, through an electronic system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

F. **Disclosure of Details of an Investigation**

If any Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law willfully and without lawful excuse or justification or in excess of a lawful excuse or justification, discloses:

i. the fact that an order has been made; or
ii. anything done under the order; or
iii. any data collected or recorded under the order;

such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

G. Failure to permit Assistance

If any person other than the suspect, wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification, fails to permit or assist a person based on an order as specified by Sections X, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

H. Harassment utilizing means of Electronic Communication

If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification,, initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person and thereby using an electronic system to support severe, repeated, and hostile behavior, such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

I. SPAM

3) If any person wilfully, without lawful excuse or justification or in excess of a lawful excuse or justification:
   i. initiates the transmission of spam; or
   ii. uses a protected electronic system to relay or retransmit spam, with the intent to deceive or mislead users, or any electronic mail or service provider, as to the origin of such messages, or
   iii. materially falsifies header information in spam and intentionally initiates the transmission of such messages,

   such a person shall be liable to the punishment with the fine not exceeding […] Rupees and with imprisonment not exceeding […] years or with both, depending on the degree of the offence.

4) **Explanation:** The transmission of single or multiple electronic messages within a customer or business relationship is not considered to be covered by Subsection (1)(i) provided that the customer did not actively reject the submission of such electronic messages prior to the transmission.

Appendix 2

Explanatory Notes to the Draft

(a) Access

While some comparable pieces of legislation in other countries limit the definition of access to acts of entering a computer system the definition included in the Bill was extracted from the Electronic Transactions Act. Based on the definition there access means an opportunity of gaining entry into, logical, arithmetical or resources of memory function of any electronic system, computer system or network. It is therefore in line with the approaches undertaken by other countries but more precise by describing the specificities of the act.

(b) Child

The term “child” on an international level is defined by Article 1 of the UN Convention of the Rights of the Child. Based on this definition a child is a person below the age of 18. However, the Childrens Act, 2048 uses a different definition. Based Sec. 2 of the Childrens Act, 2048, child includes a minor not having completed the age of sixteen years. Despite the difference to the UN Convention this definition was used in the Bill. To ensure consistancy within the legislation in case of modifications to the Childrens Act a reference to the definition could be included in the definition. Details of the determination of age, for example the question if the appearance can be used in cases where information about the real age of the child cannot be obtained, are left to interpretation by courts to determine this in accordance with the requirements of domestic laws. The definition of child pornopgraphy in this respect contains certain guidance.