

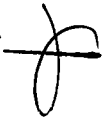
SEVENTEENTH CONGRESS OF THE REPUBLIC)
OF THE PHILIPPINES)
First Regular Session)



Senate
Office of the Secretary

'16 AUG 22 AIO :39

SENATE
S.B. No. 1051

RECEIVED BY: 

Introduced by: Senator Paolo Benigno "Bam" A. Aquino IV

AN ACT
ESTABLISHING A MAGNA CARTA FOR PHILIPPINE INTERNET FREEDOM, CYBERCRIME
PREVENTION AND LAW ENFORCEMENT, CYBERDEFENSE
AND NATIONAL CYBERSECURITY

EXPLANATORY NOTE

In today's increasingly wired and interconnected society, Internet connectivity has become more than just a luxury, and certainly more than just a tool for the educated and the elite. It is essential in the provision of basic government and private sector services, in sharing educational material information to our students, in the conduct of everyday business, and even in gathering real-time, life-saving information.

For instance, we saw during the onslaught of typhoons Ondoy and Pepeng in 2009, Sendong in 2011, Pablo in 2012, and Yolanda in 2013, how the Philippine online community worked together from behind computers and mobile phones to send crucial information about flooded areas, missing persons, areas in need of immediate rescue and relief, fundraising efforts, and many others. In an age of climate change and harsher weather conditions, being connected and "in the know" could spell the difference between life and death.

Internet-enabled platforms and services have likewise given birth to new industries, which in turn have opened up hundreds of thousands of jobs for ordinary Filipinos. The Business Process Outsourcing (SPO) and Knowledge Process Outsourcing (KPO) industries, for example, would not be able to survive without the infrastructure for secure Internet connectivity. Likewise, a growing number of freelancers, start-up entrepreneurs, online marketers, and the like have been able to find gainful employment and livelihood thanks to Internet technology. Even loan services and fundraising efforts have been powered by the Internet, making it more accessible for groups with great ideas to get the funding support that they need.

Beyond these, the Internet and social media have become integral to ensuring transparency, accountability, and good governance not only in the Philippines but also in many corners of the world. For many, the Internet represents a lifeline to citizen watchdog groups and media organizations that shine the light on truth where it is most needed.

Internet-enabled platforms have become complementary tools for democracy, allowing for debate and discourse, the free exchange of ideas, and open access to public servants. Moreover, developments in the social media space have made it possible for government to engage with its constituents on a one-to-one level, bringing government service directly in the hands of hands of the people.

It is for these reasons, and many more, that we seek to support the Magna Carta for Philippine Internet Freedom (MCPIF), in order to push for universal access to the Internet, the freedom and the ability to access public information online, freedom of speech, the right to create without fear of intellectual property infringement, and many other rights that are afforded Filipinos as citizens of a democratic republic.

Specifically, we wish to push for a provision that makes free WIFI access mandatory for designated public spaces within local government units (LGUs), such as city or municipal halls, and the like. Public WIFI access will ensure that the Internet and other digital or social media platforms may be used by LGUs and their citizens for such functions as: the provision of basic government services (e.g., business registration, the accessing of government data online, etc.); real-time monitoring and disaster response coordination during times of natural and man-made disasters; data gathering, transmission, and monitoring during local elections; online training and capacity-building, and many others.

Just as the MCPIF upholds many of our civil liberties, it likewise protects citizens' privacy online and also outlines the limitations of Internet use. The MCPIF also tackles such issues as hacking, Internet libel, hate speech, child pornography, cyber crime, human trafficking, and a host of other issues.

The world is changing at breakneck speed, and we believe that a piece of legislature such as the Magna Carta for Philippine Internet Freedom will enable us to manage the winds of change.

In view of the foregoing, the passage of this bill is earnestly sought.



Senator Paolo Benigno "Bam" A. Aquino IV



SEVENTEENTH CONGRESS OF THE REPUBLIC)
OF THE PHILIPPINES)
First Regular Session)

'16 AUG 22 A10 :39

SENATE
S.B. No. 1051

RECEIVED BY: 

Introduced by: Senator Paolo Benigno "Bam" A. Aquino IV

AN ACT
ESTABLISHING A MAGNA CARTA FOR PHILIPPINE INTERNET FREEDOM, CYBERCRIME
PREVENTION AND LAW ENFORCEMENT, CYBERDEFENSE
AND NATIONAL CYBERSECURITY

Be it enacted by the Senate and House of Representatives of the Philippines in Congress assembled:

1 **Part I. General Provisions.**

2 *Section 1. Short Title.* – This Act shall be known as “The Magna Carta for Philippine Internet
3 Freedom.”

4 *Section 2. Declaration of Policy.* –

5 (a) The State affirms that all the rights, guarantees, and privileges provided by the
6 Bill of Rights and the Constitution, as well as those established under general principles of
7 international law and under treaties and conventions to which the Philippines is a signatory,
8 shall govern in the use, development, innovation, and invention of information and
9 communications technology (ICT) and the Internet by the Filipino people.

10 (b) The State affirms its commitment to the people and to all nations that, in the
11 crafting of laws and regulations governing the use of the Internet and of ICT, these shall be
12 subject to the parameters set forth under the Constitution.

13 (c) The State reaffirms the vital role of communication and information in nation-
14 building, as stated in Article II, Section 24, of the Constitution;

15 (d) The growth of the Internet and ICT both depend on and contribute to the growth
16 of the economy, advances in science and technology, and the development of human
17 capital, and encourage democratic discourse and nation-building;

1 (e) The public and private sector have a role in the development, invention, and
2 innovation for the Internet and for ICT, through domestic, international, and transnational
3 efforts; thus, the State shall encourage development, invention, and innovation through and
4 for the Internet and ICT in cooperation with the private sector, other nations, and
5 international bodies;

6 (f) The State recognizes that network bandwidth is a finite resource that is limited by
7 technological advancements and by telecommunications infrastructure and investment;
8 thus, the State shall encourage the development of information and communications
9 technology and infrastructure;

10 (g) The Internet and ICT further enable participative governance, transparency, and
11 accountability in government; thus, the State reaffirms its policy of full public disclosure of
12 all its transactions involving public interest and to develop plans, policies, programs,
13 measures, and mechanisms using the Internet and ICT in the implementation of its policy of
14 full public disclosure;

15 (h) The State recognizes the basic right of all persons to create, access, utilize and
16 share information and knowledge through ICT, and shall promote the Internet and ICT as a
17 means for all to achieve their full potential, promote their sustainable development, and
18 improve their quality of life;

19 (i) The growth of the Internet and ICT affect peace and order and the enforcement of
20 law within the national territory and across other nations; thus, the State reaffirms its policy
21 of cooperation and amity with all nations, and its adoption of generally accepted principles
22 of international law as part of the law of the land, in the pursuit of peace and order and in
23 the enforcement of law;

24 (j) The Internet has the potential to become a theater of war, and that ICT can be
25 developed into weapons of mass destruction; thus, consistent with the national interest and
26 the Constitution, the State shall pursue a policy of "no first use" of cyberweapons against
27 foreign nations, and shall implement plans, policies, programs, measures, and mechanisms
28 to provide cyberdefense of Philippine Internet and ICT infrastructure resources; and,

29 (k) Art and culture can be created on devices, on networks, and on the Internet;
30 thus, the State shall pursue a policy that promotes the Internet and information and
31 communications technology, and the innovation therein and thereof, as instruments of life,
32 liberty, and the pursuit of happiness.

33

Part 2. Definition of Terms.

1 *Section 3. Definition of Terms.* – Whenever applicable, definitions shall be adopted from
2 those established by the International Telecommunications Union (ITU), the Internet
3 Engineering Task Force (IETF), the World Wide Web Consortium (WWWC), and the Internet
4 Corporation for Assigned Numbers and Names (ICANN), and other international and
5 transnational agencies governing the development, use, and standardization of information
6 and communications technology and the Internet. For purposes of this Act, the following
7 terms shall mean:

8 (a) Access – The ability and means to communicate with or otherwise interact with a
9 device, computer, system or network, to use resources to handle information, to
10 gain knowledge of the information the device, computer, system, or network
11 contains, or to control device or system components and functions.

12 (b) Administrator – A person or role with privileged access and control over a
13 network or a multi-user computing environment responsible for the operation and
14 the maintenance of the network or computing environment.

15 (i) Network administrator – A person or role responsible for the operation
16 and the maintenance of a network.

17 (ii) Systems administrator – A person or role responsible for managing a
18 multi-user computing environment.

19 (c) Availability – The ability of a device or set of devices to be in a state to perform a
20 required function under given conditions at a given instant of time or over a given
21 time interval, assuming that the required external resources are provided.

22 (d) Bandwidth – The capacity of a transmission medium to carry data.

23 (e) Bot – A computer program or software installed in a device, computer, computer
24 system, or network capable of performing automated tasks over the Internet,
25 without the knowledge or consent of the user or owner of the device computer,
26 system, or network, with control ceded to a third party, usually malicious. Bot may
27 also refer to the individual device that is infected with such programs or software.

28 (i) Botnet – A network of computers infected with bots.

29 (f) Cache – A temporary storage of recently accessed data or information, which may
30 be stored in the local storage medium of a device or computer, or in the storage
31 media of a network, for purposes of speeding up subsequent retrievals of data or

1 information from the Internet or networks.

2 (g) Chief Information Officer (CIO) – A third-ranking career executive in charge of the
3 information and communications technology/information technology/management
4 information systems (ICT/IT/MIS) office in a department, bureau or government-
5 owned or -controlled corporation/government financial institution, including
6 legislative, judicial and constitutional offices.

7 (h) Code – The symbolic arrangement of data or instructions in a computer program
8 or a set of such instructions.

9 (i) Component – Any individual part of a device.

10 (j) Computer – Any device or apparatus which, by electronic, electro-mechanical or
11 magnetic impulse, or by other means, is capable of receiving, recording,
12 transmitting, storing, processing, retrieving, or producing information, data, figures,
13 symbols or other modes of written expression according to mathematical and logical
14 rules or of performing any one or more of those functions.

15 (k) Computer program – A set of instructions expressed in words, codes, schemes or
16 in any other form, which is capable when incorporated in a medium that the
17 computer can read, of causing the computer to perform or achieve a particular task
18 or result.

19 (l) Configuration – The way a device, computer, computer system, or network is set
20 up.

21 (m) Content – Data that can be readily understood by a user immediately upon
22 access, which may include but is not limited to text, pictures, video, or any
23 combination thereof. The word is synonymous to information. Data that is readable
24 and usable only by and between devices, computers, systems or networks, such as
25 traffic data, is not content.

26 (n) Control – The use of resources, modification of the configuration, and otherwise
27 exertion of a directing influence on the operation of a device, computer, system, or
28 network.

29 (o) Critical infrastructure – The systems and assets, whether physical or virtual, so
30 vital to the Philippines that the incapacity or destruction of such systems and assets
31 would have a debilitating impact on national security, economy, public health or
32 safety, or any combination of those matters.

1 (p) Critical network – An information and communications system or network of
2 systems, whether physical or virtual, so vital to the Philippines that the incapacity or
3 destruction of such a network would have a debilitating impact on national security,
4 economy, public health or safety, or any combination of those matters.

5 (q) Cryptography – The discipline which embodies principles, means, and methods
6 for the transformation of data in order to hide its information content, prevent its
7 undetected modification and/or prevent its unauthorized use.

8 (r) Cyber environment – The environment comprised of users, networks, devices, all
9 software, processes, information in storage or transit, applications, services, and
10 systems that can be connected directly or indirectly to networks or the Internet.

11 (s) Cyberattack – An attack by a hostile foreign nation-state or violent non-state
12 actor on Philippine critical infrastructure or networks through or using the Internet
13 or information and communications technology. The term may also be used to mean
14 an assault on system security that derives from an intelligent threat, *i.e.*, an
15 intelligent act that is a deliberate attempt to evade security services and violate the
16 security policy of a system.

17 (t) Cybercrime – Any unlawful act punishable by this law or other relevant laws
18 committed through or using the Internet or information and communications
19 technology.

20 (u) Cyberdefense – The collection of plans, policies, programs, measures,
21 mechanisms, and weapons designed to defend the Philippines from cyberattack.

22 (v) Cyberintelligence – The collection, analysis, processing, and dissemination of
23 information, which may be done through or using the Internet or information and
24 communications technology, designed to provide guidance and direction to
25 commanders and leaders of military and law enforcement units towards the
26 combating of acts of cyberattack and cyberterrorism.

27 (w) Cybersecurity – The collection of tools, policies, security concepts, security
28 safeguards, guidelines, risk management approaches, actions, training, best
29 practices, assurance, and technologies that can be used to protect the cyber
30 environment and organization and user's information and communications
31 technology assets.

32 (x) Cyberspace – A global domain within the information environment consisting of

1 the interdependent network of information systems infrastructures including the
2 Internet, telecommunications networks, computer systems, and embedded
3 processors and controllers, or the virtual space constituted by a computer network
4 with a set of distributed applications and its users.

5 (y) Cyberterrorism – A violation of the Human Security Act of 2007 committed
6 through or using the Internet or information and communications technology.

7 (z) Cyberwarfare – The damaging, disruptive, saboteurish, or infiltrative actions, or
8 analogous acts of a belligerent nature, by a nation-state or violent non-state actor
9 against the Philippines, its government, or its citizens, with the intent to cause
10 damage and disruption to the people, property, infrastructure, or systems of the
11 Philippines, through or using computers, information and communications
12 technology, networks, or the Internet.

13 (aa) Data – The reinterpretable representation of information in a formalized
14 manner suitable for communication, interpretation, or processing, or information
15 represented in a manner suitable for automatic processing.

16 (i) Data, private – Any and all data that does not fall under the definition of
17 public data.

18 (ii) Data, public – Data which is available to the public without access being
19 restricted by requirements of membership, non-disclosure agreements or similar.

20 (iii) Data, traffic – Data that is readable and usable only solely by and
21 between devices, computers, systems or networks, used for purposes of facilitating
22 the transfer of information between devices, computers, systems or networks.

23 (ab) Device – The material element or assembly of such elements intended to
24 perform a required function.

25 (ac) Download – The transfer of data or information from the Internet or a network
26 to a device or computer upon request of the user for this information.

27 (ad) Encryption – An encoding scheme that produces meaningless information to all
28 observers except those with the decryption key made for the purpose.

29 (ae) End user license agreement – The legal agreement between two parties, one of
30 which is the user, that stipulates the terms of usage of a device, software, or service.

1 (af) Equipment – A single apparatus or set of devices or apparatuses, or the set of
2 main devices of an installation, or all devices necessary to perform a specific task.

3 (i) Data processing equipment – Equipment used to process data
4 electronically.

5 (ii) Network equipment – Equipment used to allow data communication
6 between devices, computers, systems, networks, or the Internet.

7 (iii) Storage equipment – Equipment used to store data in an electronic form,
8 and allow the retrieval of data by electronic means.

9 (ad) Executable – The ability of a code, script, software, or computer program to be
10 run from start to finish in a device or computer, and providing a desired result.

11 (ae) Free and open-source software – Liberally licensed software whose license
12 grants users the right to use, copy, study, change, and improve its design through
13 the availability of its source code.

14 (af) Hardened – The state of reduced vulnerability to unauthorized access or control
15 or to malicious attacks of a device, computer, network, or information and
16 communications technology infrastructure.

17 (ag) Hardware – The collection of physical elements that comprise a device,
18 equipment, computer, system, or network.

19 (ah) High-speed connection – A service that provides data connection to networks
20 and the Internet that has data rates faster than what is generally available to the
21 general public.

22 (ai) High-volume connection – A service that provides data connection to the
23 networks and the Internet that allows volumes of uploadable and/or downloadable
24 data larger than what is generally available to the general public.

25 (aj) Information – Data that can be readily understood by a user immediately upon
26 access, which may include but is not limited to text, pictures, video, or any
27 combination thereof. The word is synonymous to content. Data that is readable and
28 usable only by and between devices, computers, systems or networks, such as traffic
29 data, is not information.

1 (i) Private information – Refers to any of these three classes of information:

2 (1) any information whether recorded in a material form or not, from
3 which the identity of an individual is apparent or can be reasonably and
4 directly ascertained by the entity holding the information, or when put
5 together with other information would directly and certainly identify an
6 individual;

7 (2) Any and all forms of data which under the Rules of Court and other
8 pertinent laws constitute privileged communication; and,

9 (3) any information whose access requires the grant of privileges by a
10 duly-constituted authority, which may include but is not limited to a systems
11 or network administrator.

12 (ii) Sensitive private information – Refers to personal information:

13 (1) About an individual's race, ethnic origin, marital status, age, color,
14 and religious, philosophical or political affiliations;

15 (2) About an individual's health, education, genetic or sexual life of a
16 person, or to any proceeding for any offense committed or alleged to have
17 been committed by such person, the disposal of such proceedings, or the
18 sentence of any court in such proceedings;

19 (3) Issued by government agencies peculiar to an individual which
20 includes, but not limited to, social security numbers, previous or current
21 health records, licenses or its denials, suspension or revocation, and tax
22 returns; and

23 (4) Specifically established by an executive order or an act of Congress
24 to be kept classified.

25 (iii) Public information – Any information that is not restricted by virtue of the
26 preceding definitions and can be readily accessed by any interested member of the
27 public.

28 (ak) Information and communications technology – The integration of real-time
29 communication services, non-real-time communication services, and
30 telecommunications, computers, software, hardware, storage, and devices, which
31 enable users to access, store, transmit, and manipulate information.

1 (al) Internet – The global system of interconnected computer networks linked by
2 various telecommunications technologies and that uses the standard Internet
3 protocol suite.

4 (am) Medium – A material used for specific purposes.

5 (i) Storage medium – The physical material or device in which data or
6 information may be stored, which includes but is not limited to magnetic tape, disk
7 drives, flash devices, electrically erasable programmable read-only memory
8 (EEPROM) chips, optical media disks, punched cards, and paper.

9 (ii) Transmission medium – The physical material through which a data
10 communication signal is transmitted, which includes but is not limited to twisted-
11 pair copper wire, coaxial cable, optical fiber, and air.

12 (an) Network – A collection of computers, devices, equipment, and other hardware
13 interconnected by communication channels that allow sharing of resources and
14 information.

15 (i) Open network – A network, such as the Internet, which allows any entity
16 or device to interconnect with freely at any time and become a user or part of the
17 network, provided the entity or device uses the same or compatible communications
18 protocols, and which allows any user to cease interconnectivity with freely at any
19 time, provided the user does so in a manner that does not compromise the security
20 protocols of the open network or of other users.

21 (ii) Private network – A network which is operationally private by nature and
22 not universally accessible by the general public.

23 (iii) Public network - A network which provides services to the general public.

24 (ao) Offline – The state of being disconnected from the Internet or networks.

25 (ap) Online – The state of being connected to the Internet or a network.

26 (aq) Ownership – Ownership is defined by the Civil Code.

27 (i) Privately-owned – Ownership as provided for by the Civil Code of the
28 Philippines by a natural person or a juridical person under Article 44 paragraph (3) of
29 the Civil Code.

1 (ii) Publicly-owned – Ownership as provided for by the Civil Code of the
2 Philippines by a juridical person under Article 44 paragraphs (1) and (2) of the
3 Civil Code.

4 (ar) Physical plant – The building, structure, and infrastructure necessary to support
5 and maintain a facility.

6 (as) Platform – The hardware architecture and/ or software framework, including
7 application frameworks, whose combination allows a user to run software.

8 (at) Privacy – May refer to any of these definitions, or a combination of these
9 definitions:

10 (i) the right guaranteed and protected by the Constitution;

11 (ii) the right of individuals to control or influence what personal information
12 related to them may be collected, managed, retained, accessed, and used or
13 distributed;

14 (iii) the protection of personally identifiable information; and,

15 (iv) a way to ensure that information is not disclosed to anyone other than
16 the intended parties (also known as "confidentiality").

17 (au) Privilege – A right that, when granted to an entity, permits the entity to perform
18 an action.

19 (i) Privileged access – The completely unrestricted access of a user to the
20 resources of a device, computer, system, or network.

21 (ii) Privileged control – The completely unrestricted ability of a user to use
22 the resources, modify the configuration, and otherwise exert a directing influence on
23 the operation of a device, computer, system, or network.

24 (av) Processing – The act of performing functions or activities on data or information.

25 (i) Processing (Data Privacy Act) – Any operation or any set of operations
26 performed upon personal information including, but not limited to, the collection,
27 recording, organization, storage, updating or modification, retrieval, consultation,
28 use, consolidation, blocking, erasure or destruction of data. (RA 10173)

1 (ii) Data processing – Any process to enter data and summarize, analyze or
2 otherwise convert data into usable information.

3 (iii) Information processing – The transformation of information in one form
4 to information in another form through an algorithmic process.

5 (aw) Protocol – A defined set of procedures adopted to ensure communication, or a
6 set of rules for data transmission in a system interlinking several participants.

7 (ax) Publication – The act of making works available to the public by wire or wireless
8 means in such a way that interested members of the public may access these works
9 from a place and time individually chosen by them.

10 (ay) Script – A computer program or sequence of instructions that is interpreted or
11 carried out by another computer program instead of directly by a computer, device,
12 or equipment.

13 (az) Security – The ability to prevent fraud as well as the protection of information
14 availability, integrity and confidentiality.

15 (i) Security, behavioral – The use of laws, regulations, policies, procedures,
16 instructions and the like to influence or restrict behavior for purposes of maintaining
17 security.

18 (ii) Security, electronic – The use of computer programs, software, code,
19 scripts, devices, or equipment for purposes of maintaining security.

20 (iii) Security, physical – The use of locks, gates, security guards, and other
21 analogous means, for purposes of maintaining security.

22 (ba) Service – A set of functions offered to a user by another person or by an
23 organization.

24 (bb) Service quality – The collective effect of service performance which determines
25 the degree of satisfaction of a user of the service.

26 (bc) Software – The set of programs, procedures, algorithms and its documentation
27 concerned with the operation of a data processing system, computer, device, or
28 equipment.

1 (bd) Software application – Software designed to help a user perform a specific task
2 or set of tasks.

3 (be) State - The Republic of the Philippines, any of its political subdivisions,
4 departments and agencies, including but not limited to government owned or
5 controlled corporations or government corporate entities.

6 (bf) Telecommunications – A service or system of interconnected entities providing
7 the ability to exchange and interchange data between points or from a point to
8 multiple points.

9 (bg) Universal access - The provision of adequate and reliable facilities at reasonable
10 charges in all areas within Philippine jurisdiction, as far as is technologically sound
11 and practicable and subject only to technological and reasonable economic
12 limitations, without any discrimination on the basis of gender, sexual orientation,
13 religious belief or affiliation, political belief or affiliation, ethnic or regional affiliation,
14 citizenship, or nationality.

15 (bh) Upload – The transfer of data or information to the Internet or a network from a
16 device or computer, initiated by the user.

17 (bi) Uptime – The time a device, equipment, computer, or network can be left
18 unattended without suffering failure, or needing to be undergo administrative or
19 maintenance purposes.

20 (bj) User – Any person, whether natural or juridical, or any entity that makes use of a
21 part or whole of the resources of a device, equipment, computer, system, network,
22 software, software application, code, or script.

23 (bk) Virus – Any computer program, code, or script that implements unauthorized
24 and/or undesirable changes to a device, computer, equipment, system, or network.
25 For purposes of this Act, the term may be used synonymously with malware,
26 spyware, worms, trojans, and the like.

27 **Part 3. Internet Rights and Freedoms**

28 *Section 4. Right to Freedom of Speech and Expression on the Internet. –*

29 (a) The State shall, within its jurisdiction:

30 (i) Protect and promote the freedom of speech and expression on the

1 Internet;

2 (ii) Protect the right of the people to petition the government via the Internet
3 for redress of grievances;

4 (iii) Protect the right of any person to publish material on or upload
5 information to the Internet; and,

6 (iv) Not promote censorship or the restriction of the viewing of any content
7 on the Internet, until after the issuance of an appropriate Order pursuant to the
8 provisions of this Section

9 (b) A person's right to publish content on the Internet, or to remove one's own
10 published content or uploaded data, is recognized as integral to the constitutional right to
11 free expression and shall not be subject to any licensing requirement from the State.

12 (c) Any State action that constitutes prior restraint or subsequent punishment in
13 relation to one's Internet's rights shall be authorized only upon a judicial order issued in
14 conformity with the procedure provided under Section 5 of this Act. Provided, that
15 notwithstanding Section 5, any such judicial order issued upon motion of the Republic of the
16 Philippines, any of its political subdivisions or agencies including government-owned or
17 controlled corporations, shall be issued only upon the following grounds:

18 (i) the nature of the material or information subject of the Order creates a
19 clear and present danger of a substantive evil that the state has a right or duty to
20 prevent;

21 (ii) the material or information subject of the Order is not protected
22 expression under the standards of the community or the audience toward which the
23 material or information is directed; and

24 (iii) the publication of the material or the uploading of the information
25 subject of the Order will constitute a criminal act punishable by laws enumerated in
26 Section 5 of this Act.

27 (d) No person shall be compelled to remove published content or uploaded data
28 from the Internet that is beyond the said person's capacity to remove. The party seeking to
29 compel the removal of the content or data has the burden to prove that the person being
30 compelled has the capacity to remove from the Internet the specific content or data. For
31 purposes of this section, content or data retained in web archives or mirror sites are
32 presumed to be content and data that is beyond the capacity of the person being compelled

1 to remove.

2 *Section 5. Promotion of Universal Access to the Internet. –*

3 (a) The State shall, within its jurisdiction, protect and promote universal access to
4 the Internet.

5 (b) A person's right to unrestricted access to the Internet may, upon discretion of the
6 appropriate Cybercrime Court whose jurisdiction is defined in this Act, be suspended as an
7 accessory penalty upon final conviction for any of the following criminal offenses:

8 (i) The felonies of robbery, theft, estafa, falsification, malversation, and
9 usurpation of authority or official functions, as defined in appropriate penal laws,
10 committed by through or using the Internet or information and communications
11 technology;

12 (ii) Any criminal offense defined and punishable in the following special penal
13 laws: the Anti-Trafficking in Persons Act of 2003 (RA 9208), the Anti-Graft and
14 Corrupt Practices Act, the Code of Conduct and Ethical Standards for Public Officials
15 and Employees (RA 6713), the Anti-Money Laundering Act of 2001 (RA 9160), the
16 Violence Against Women and Children Act (RA 9262), the Special Protection of
17 Children Against Abuse, Exploitation, and Discrimination Act (RA 7610), the Child and
18 Youth Welfare Code (PD 603), the Anti-Child Pornography Act of 2009 (RA 9775), the
19 Human Security Act of 2007 (RA 9732), or the Data Privacy Act of 2012 (RA 10173),
20 committed through or using the Internet or information and communications
21 technology; or

22 (iii) Any criminal offense defined and punishable by this Act.

23 The right of person accused of any of the above offenses to unrestricted access to
24 the Internet may be suspended or limited by the court of competent jurisdiction pending
25 final judgment upon a showing, following notice and hearing, that there is a strong
26 likelihood that the accused will be able to facilitate the commission of the offense so
27 charged unless such order were issued.

28 (c) It is presumed that all persons have the right to unrestricted access to the
29 Internet, subject to the parameters established under this Act. Any voluntary restriction or
30 waiver of such right must be established by preponderance of evidence.

31 Any final judicial relief that seeks to limit or suspend, in whole or in part, one's right
32 to unrestricted access to the Internet, shall be determined in accordance with the

1 appropriate law, including but not limited to the Civil Code and this Act. Any civil action that
2 seeks as a relief, in part or in whole, the limitation or suspension of a person's right to
3 unrestricted access to the Internet, shall be filed exclusively with the Cybercrime Courts.

4 No court shall issue any provisional Order suspending the right to unrestricted access
5 to the Internet of any person without prior notice and hearing, and only upon the grounds
6 for the issuance of a preliminary injunction under the Rules of Court.

7 (d) The authority of the State to suspend one's right to unrestricted Internet access
8 is confined solely to the courts of competent jurisdiction and may not be exercised by any
9 government agency, notwithstanding any contrary provisions of law. The right of the State
10 to infringe a person's right to unrestricted Internet access shall be governed by Section 5 of
11 this Act.

12 (e) No person or entities offering Internet access for free, for a fee, or as an extra
13 offering separate from the services already being offered, including but not limited to any
14 hotel, restaurant, commercial establishment, school, religious group, organization, or
15 association, shall restrict access to the Internet or any other public communications network
16 from within its private network, or limit the content that may be accessed by its employees,
17 students, members, or guests, without a reasonable ground related to the protection of the
18 person or entity from actual or legal threats, the privacy of others who may be accessing the
19 network, or the privacy or security of the network as provided for in the Data Privacy Act of
20 2012 (RA 10173) and this Act.

21 (f) The State, through the Department of Information and Communication
22 Technology, in coordination with the Department of Tourism and the Local Government
23 Units, shall provide free WIFI access in designated public areas. These public areas may
24 include but not be limited to the following:

- 25 (i) common areas of local government offices;
- 26 (ii) train stations;
- 27 (iii) bus stations;
- 28 (iv) tourism spots;
- 29 (v) heritage spots; and
- 30 (vi) public parks.

31 *Section 6. Right to Privileged Access To and Control of Devices. –*

32 (a) The State shall, within its jurisdiction, protect the right of a person to gain or
33 attain privileged access or control over any device over which the person has property
34 rights.

1 (b) Any person involved in the wholesale or retail of devices may install, implant, or
2 otherwise put in a device a component, a configuration, or code that shall restrict the
3 operation of a device; *Provided*, the installation or implantation is for the sole purpose of
4 ensuring the privacy or security of the interconnection or interoperability of the device with
5 public or private networks or Internet or information and communications technology
6 infrastructure; *Provided further*, that notice is provided to potential buyers of the device of
7 the presence of the component, configuration, and code; *Provided further*, that the buyer
8 may request the removal or modification of the component, configuration, or code prior to
9 purchase from the seller and shall assume all risks attendant to such removal or
10 modification. Removal or modification of the component, configuration, or code by any
11 person except the seller, manufacturer, or duly authorized representative may be cause for
12 a waiver of the warranty of the device.

13 (c) Unless otherwise provided by law, any person who has property rights over any
14 device may, by physical, electronic, or any other means, gain or attain privileged access or
15 control to such device; *Provided*, the gain or attainment of privileged access or control was
16 not intended to circumvent the protection of or cause the actual infringement on
17 intellectual property rights of another person.

18 *Section 7. Protection of the Freedom to Innovate and Create Without Permission. –*

19 (a) The State shall, within its jurisdiction, protect and promote the freedom to
20 innovate and create without need for permission. No person shall restrict or deny another
21 person the right to develop new information and communications technologies, without
22 due process of law or authority vested by law.

23 (b) Subject to such conditions as provided for in the Intellectual Property Code and
24 other relevant laws, no person shall be denied access to new information and
25 communications technologies, nor shall any new information and communications
26 technologies be blocked, censored, suppressed, or otherwise restricted, without due
27 process of law or authority vested by law.

28 (c) No person who shall have created, invented, innovated, or otherwise developed a
29 new information and communications technology shall be penalized for the actions of the
30 users of the new information and communications technology.

31 *Section 8. Right to Privacy of Data. –*

32 (a) The State shall, within its jurisdiction, promote the protection of the privacy of
33 data for all persons.

1 (b) Any person shall have the right to employ means such as encryption or
2 cryptography to protect the privacy of the data or networks which such person owns or
3 otherwise possesses real rights over.

4 (c) Subject to such conditions as provided for in the Data Privacy Act of 2012 (RA
5 10173) and other relevant laws, no person shall access the private data of another person.

6 (d) The State shall, within its jurisdiction, guarantee a person's right of privacy over
7 his or her data or network rights, and such person's rights employ reasonable means to
8 protect such right of privacy.

9 (e) The State is required to ensure the appropriate level of privacy of the data and of
10 the networks maintained by it. Failure to do so shall be penalized by this Act and other
11 relevant laws.

12 (f) Except upon a final ruling from the courts, issued in accordance with this act, no
13 person may compel an agency or instrumentality of the State maintaining data or networks
14 to reduce the level of privacy of the data or of the networks.

15 *Section 9. Right to Security of Data. –*

16 (a) The State shall, within its jurisdiction, promote the protection of the security of
17 data for all persons.

18 (b) Any person shall have the right to employ means, whether physical, electronic, or
19 behavioral, to protect the security of his or her data or networks over which the person has
20 ownership.

21 (c) No third party shall be granted access to the private data or networks of a person
22 by an Internet service provider, telecommunications entity, or such person providing
23 Internet or data services, except upon a final court order issued in accordance with Section
24 5 of this Act. It shall be a condition precedent to the filing of such action for access to
25 private data that the person owning such data be first properly notified of such a request by
26 the Internet service provider, telecommunications entity, or such person providing Internet
27 or data services, and that such person has refused to grant the requested access. A person
28 shall not be deemed to have been properly notified unless the person has acknowledged
29 the notification of the request for access and has agreed to grant or refuse access.

30 (d) No third party granted the right to access the private data or networks of a
31 person by an Internet service provider, telecommunications entity, or other such person

1 providing Internet or data services, shall be given any property rights over the data being
2 accessed, the media where the private data is stored, the equipment through which the
3 network is run or maintained, or the physical plant where the network equipment is
4 housed, beyond the right to access the private data or network, unless otherwise granted
5 such rights by the courts following the appropriate action and final order.

6 (e) No person shall be deprived of his or her device, network equipment, or physical
7 plant that may be the subject of an appropriate complaint filed in connection with this Act,
8 except:

9 (ii) Upon a lawful warrant issued in connection with the appropriate criminal
10 case by the courts in accordance with the Rules of Court; *Provided*, that there must
11 first be a determination from the courts that the data, information, or contents
12 cannot be separated from the device, network equipment, or physical plant; and,

13 (ii) Upon a final decision by the courts issued in accordance with Section 5 of
14 this Act.

15 (f) The State shall be required to ensure the appropriate level of security of the data
16 and of the networks, whether private or public, that it maintains. Failure to do so shall be
17 penalized by this Act and other relevant laws.

18 (h) It shall be unlawful for any person to compel an agency or instrumentality of the
19 State maintaining data or networks to reduce the level of security of the data or of the
20 networks being maintained.

21 *Section 10. Protection of Intellectual Property. –*

22 (a) The State shall, within its jurisdiction, protect the intellectual property published
23 on the Internet of all persons, in accordance with the Intellectual Property Code of the
24 Philippines (RA 8293), as amended, and other relevant laws.

25 (b) It shall be presumed that any content published on the Internet is copyrighted,
26 unless otherwise explicitly provided for by the author, subject to such conditions as
27 provided for in the Intellectual Property Code of the Philippines (RA 8293), as amended, and
28 other relevant laws.

29 (c) Subject to the Intellectual Property Code of the Philippines (RA 8293), as
30 amended, and other relevant laws, no Internet service provider, telecommunications entity,
31 or such person providing Internet or data services shall have intellectual property rights
32 over derivative content that is the result of creation, invention, innovation, or modification

1 by a person using the service provided by the Internet service provider, telecommunications
2 entity, or such person providing Internet or data services, unless such content is a derivative
3 work of content already owned by or assigned to the Internet service provider,
4 telecommunications entity, or such person providing Internet or data services acting as a
5 content provider. The exception to the intellectual property rights of the person must be
6 explicitly provided for via an end user license agreement to which both parties have agreed,
7 and the existence of the derivative content must be dependent on the service provided by
8 the Internet service provider, telecommunications entity, or such person providing Internet
9 or data services.

10 (d) Notwithstanding existing provisions of law, it shall be presumed that the parents
11 or guardians of a minor shall have provided agreement and shall be bound to the terms of
12 an end user license agreement should the minor in their care signify agreement to the end
13 user license agreement.

14 (e) Notwithstanding existing provisions of law, it shall be presumed that any
15 infringement of intellectual property rights by a minor was done with the knowledge and
16 consent of his parents or guardians.

17 *Section 11. Protection of the Internet as an Open Network. –*

18 (a) The State shall, within its jurisdiction, protect and promote the Internet as an
19 open network.

20 (b) No person or entity shall restrict or deny the interconnection or interoperability
21 of a device, an equipment, or a network that is capable of such interconnection or
22 interoperability to the Internet, to other public networks, or to other Internet service
23 providers, telecommunications entities, or other such persons providing Internet or data
24 services, without due process of law or authority vested by law. *Provided*, Customer
25 premises equipment as redefined by this Act, shall not be covered by the requirements
26 under this Section. *Provided, further*, The interoperability of a device, an equipment, or a
27 network within a private network may be restricted by the duly authorized system and/or
28 network administrators of the private network, subject to the provisions of the Data Privacy
29 Act of 2012 (RA 10173) and other relevant laws.

30 *Section 12. Promotion of network neutrality. –* No person or entity shall restrict the flow of
31 data or information on the Internet on the basis of content, nor shall any person institute
32 and employ means or methods to favor the flow of information on the Internet of one class
33 of data or information over another on the basis of content, except:

34 (a) if the data or information whose flow is being favored is used to solely to manage

1 the security or service quality of a network, or of an Internet or data service, and;

2 (b) the data or information whose flow is being favored cannot be used for any other
3 purpose other than the management of security or service quality of the network.

4 *Section 13. Promotion of the Use of the Internet and Information and Communications*
5 *Technology for Purposes of Transparency in Governance and Freedom of Information. -*

6 (a) The State recognizes that the Internet and ICT can facilitate the dissemination of
7 information and the promotion of transparency in governance. Therefore, subject to the
8 provisions of the Data Privacy Act of 2012 (RA10173) and applicable laws on government
9 information classification, the State shall, within practicable and economically reasonable
10 limits, provide for and maintain a system that shall allow the public to view and download
11 public information on plans, policies, programs, documents, and records of government.

12 (b) The State shall publish and make available for download, in readily processed
13 formats, such as plain text documents, comma-separated values spreadsheets, or open
14 standard multimedia data, and its authenticity readily verifiable through a checksum
15 standard as determined by the Internet Engineering Task Force or a similar globally
16 recognized standards organization, the following government public information, in the
17 interest of transparency and good governance:

18 (i) Audited financial statements, and budget and expenditure records;

19 (ii) Statements of assets, liabilities, and net worth, as prescribed by the Code
20 of Conduct and Ethical Standards of Public Officials and Employees (RA 6713);

21 (iii) Performance review results, as prescribed by the Anti-Red Tape Act of
22 2007 (RA 9485) and other relevant laws;

23 (iv) Laws, rules, regulations, memorandum circulars and orders, letters of
24 instruction, office orders, and other executive issuances required to be published in
25 the Official Gazette or submitted to the Office of the National Administrative
26 Registrar, or which are essential to the performance of duties of public officials and
27 employees; and,

28 (v) Other such information of the State that does not fall within any valid
29 claim of executive privilege.

30 (c) The State shall ensure that any format used for the files available for download
31 are in common use, platform independent, machine readable, or is based on an underlying

1 open standard, developed by an open community, affirmed and maintained by a standards
2 body and such open standard must be fully documented and publicly available. Such files
3 must be:

4 (i) In easily processed formats, such as plain text documents, comma-
5 separated values spreadsheets, and open multimedia formats;

6 (ii) Without restrictions that would impede the re-use of that information;
7 *Provided*, that the State shall not be precluded from charging reasonable fees to
8 cover the cost of organizing, maintaining, and publishing such information; *Provided*
9 *further*, that the State shall not be precluded from publishing the information in
10 supplemental file formats as the public may so request; and,

11 (ii) Have their authenticity verifiable through a checksum standard
12 determined by the Internet Engineering Task Force or similar globally reputable
13 organization.

14 The Bureau of Product Standards of the Department of Trade and Industry shall be
15 responsible for setting the standards for the file formats to be used by the State in the
16 publication of government public information, in accordance with the provisions of this Act.

17 (d) The State shall maintain websites or applications with mechanisms to allow for
18 the public to provide feedback, lodge complaints, or report instances of malfeasance or
19 misfeasance. Such mechanisms shall not disallow anonymous feedback, complaints, or
20 reports, and the State shall take appropriate steps to protect persons making feedback,
21 complaints, or reports from retaliation or persecution.

22 **Part 4. Regulations for the Promotion of Internet Rights and Freedoms.**

23 *Section 14. Declaration of Compliance with Treaty Obligations and International* 24 *Conventions. –*

25 (a) The State recognizes that the Internet itself is possible through the
26 standardization of units across multiple jurisdictions.

27 (b) The standards for networks and the Internet, as set by the International
28 Telecommunications Union (ITU), the Internet Engineering Task Force (IETF), the World
29 Wide Web Consortium (WWWC), and the Internet Corporation for Assigned Numbers and
30 Names (ICANN), and their successors-in-interest are hereby adopted. No agency or
31 instrumentality of the State shall issue rules and regulations contrary to these.

1 (c) The State recognizes that the rights and obligations in the use of networks and
2 the Internet that shall be guaranteed and imposed by this Act are subject to its treaty
3 obligations and obligations under instruments of international law.

4 (d) The State reaffirms its compliance to the treaties and international conventions
5 to which it is a signatory, to wit, the International Covenant on Civil and Political Rights
6 (ICCPR), the International Covenant on Economic, Social, and Cultural Rights (ICESCR), the
7 Convention on the Rights of the Child (CRC), the Convention on the Elimination of All Forms
8 of Racial Discrimination (ICERD), the Convention on the Elimination of All Forms of
9 Discrimination Against Women (CEDAW), the Convention on the Rights of Persons with
10 Disabilities (CRPD), the United Nations Convention against Transnational Organized Crime,
11 the United Nations Convention against Corruption, the Geneva Convention, the United
12 Nations Convention on Certain Conventional Weapons, the Rome Statute of the
13 International Criminal Court, the Convention on Cybercrime (Budapest Convention), and the
14 General Agreement on Tariffs and Trade (GATT), among others. No agency or
15 instrumentality of the State shall issue rules and regulations governing the use of networks
16 and the Internet contrary to these.

17 (e) The State shall keep abreast with and be guided by developments of the Internet
18 and of information and communications technology under international law and shall
19 continually design and implement policies, laws, and other measures to promote the
20 objectives of this Act.

21 *Section 15. The State as the Primary Duty Bearer.* – The State, as the primary duty-bearer,
22 shall uphold constitutional rights, privileges, guarantees, and obligations in the
23 development and implementation of policies related to the Internet and information and
24 communication technology. The State shall fulfill this duty through law, policy, regulatory
25 instruments, administrative guidelines, and other appropriate measures, including
26 temporary special measures.

27 *Section 16. Duties of the State Agencies and Instrumentalities.* –

28 (a) *Internet and Information and Communications Technology Policy.* – Subject to
29 provisions of this Act, the Department of Information and Communications Technology shall
30 be the lead agency for oversight over the development and implementation of plans,
31 policies, programs, measures, and mechanisms in the use of the Internet and information
32 and communications technology in the Philippines.

33 (b) *Cybercrime Law Enforcement.* – Subject to provisions of this Act, the Department
34 of Justice, The Department of Interior and Local Government, the Department of Social
35 Welfare and Development, the Department of Information and Communications

1 Technology, the National Bureau of Investigation, and the Philippine National Police shall be
2 jointly responsible over the development and implementation of plans, policies, programs,
3 measures, and mechanisms for cybercrime law enforcement in the Philippines.

4 (c) *Cyberdefense and National Cybersecurity.* – Subject to provisions of this Act, the
5 Department of National Defense shall be the lead agency for oversight over the
6 development and implementation of plans, policies, programs, measures, mechanisms, and
7 weapons for national cyberdefense and cybersecurity.

8 (d) *Information and Communications Technology Infrastructure Development.* –

9 (i) Subject to provisions of this Act, the Department of Information and
10 Communications Technology shall have responsibility to develop and implement
11 plans, policies, programs, measures, and mechanisms for the development of
12 information and communications technology infrastructure in the Philippines and
13 the promotion of investment opportunities to this end.

14 (ii) ICT infrastructure and facilities, including the civil works components
15 thereof, fall within private sector infrastructure or development projects as defined
16 under Republic Act No. 6957, as amended by Republic Act No. 7718, and may, upon
17 the discretion of the National Government or local government units, be the subject
18 of the contractual arrangements authorized under the said law. *Provided,* that the
19 DICT shall be the implementing agency of such projects to be implemented by the
20 national government; *Provided, further,* that the DICT shall have the right to require
21 its prior concurrence to such projects implemented by local government units,
22 through duly promulgated regulations that specify, among others, the requisite
23 threshold contract prices that would require prior concurrence of the DICT.

24 (iii) The procurement by the national government or by local governments of
25 ICT-related goods and services which will not be implemented under Republic Act
26 No. 6957, as amended by Republic Act No. 7718, shall be governed by Republic Act
27 No. 9184.

28 (iv) The development and operation of information and communications
29 technology infrastructure and facilities is hereby declared as a preferred area of
30 investment and shall be included in the annual Investment Priority Plan issued in
31 accordance with the Omnibus Investments Code. Subject to the contrary factual
32 determination of the Board of Investments, an entity involved in the development
33 and operation of information and communications technology infrastructure and
34 facilities is presumed to be entitled to register as a registered enterprise under the
35 Investment Priorities Plan; *Provided,* that an enterprise that proposes to operate a

1 public utility or public service shall be subject to the equity requirements imposed by
2 the Constitution and by applicable laws; *Provided, further,* that any such entity which
3 intends to operate in a special economic zone or in a tourism economic zone as
4 defined by applicable law shall be entitled to receive the additional investment
5 incentives granted to such zone-registered enterprises in accordance with the
6 applicable law; *Provided, finally,* that nothing in this Section shall be construed to
7 limit the available incentives to which an entity may be entitled to under Republic
8 Act No. 6957, as amended.

9 (v) The implementing rules of the registration of the entity involved in the
10 development or operation information and communications technology as well as
11 the incentives provided herein shall be developed by the Board of Investments
12 together with the DICT and the Department of Finance.

13 (vi) Subject to joint oversight by the DICT, the DOF, the Department of
14 Budget and Management, and the Commission on Audit, the NEDA may establish a
15 venture capital corporation to encourage research and development of information
16 and communications technology in the Philippines.

17 (e) *Human Resources, Skills and Technology Development for Information and*
18 *Communications Technology.* – Subject to provisions of this Act, the Department of
19 Information and Communications Technology, the Department of Science and Technology,
20 and the Technical Education and Skills Development Authority shall have the joint
21 responsibility to develop and implement plans, policies, programs, measures, and
22 mechanisms for the development of human resources, skills development, and technology
23 development for information and communications technology infrastructure in the
24 Philippines.

25 (f) *Information and Communications Technology Education.* – Subject to provisions
26 of this Act, the Department of Information and Communications Technology, the
27 Department of Education, and the Commission on Higher Education shall have the joint
28 responsibility to develop and implement plans, policies, programs, measures, and
29 mechanisms for information and communications technology education in the Philippines.

30 (g) *Intellectual Property Rights Protection in Cyberspace.* – Subject to provisions of
31 this Act and other relevant laws, the Intellectual Property Office shall, within Philippine
32 jurisdiction, be primarily responsible for the protection of intellectual property rights in
33 cyberspace. As official registrar and repository of copies of published works, the National
34 Library and the National Archives shall assist the Intellectual Property Office in the
35 protection of copyright.

1 *Section 17. Amendments to the Public Telecommunications Policy Act of the Philippines. –*

2 (a) Jurisdiction over the provision and regulation of Internet and information and
3 communications technology services shall be vested with the National Telecommunications
4 Commission, in accordance with the succeeding provisions.

5 (b) Article III, Section 5 of Public Telecommunications Policy Act of the Philippines
6 (RA 7925) is hereby amended to read:

7 *Section 5. Responsibilities of the National Telecommunications Commission. -*
8 The National Telecommunications Commission (Commission) shall be the principal
9 administrator of this Act and as such shall take the necessary measures to
10 implement the policies and objectives set forth in this Act. Accordingly, in addition to
11 its existing functions, the Commission shall be responsible for the following:

12 a) Adopt an administrative process which would facilitate the entry of
13 qualified service providers and adopt a pricing policy which would generate
14 sufficient returns to encourage them to provide basic telecommunications,
15 **NETWORK, AND INTERNET** services in unserved and underserved areas;

16 b) Ensure quality, safety, reliability, security, compatibility and inter-
17 operability of telecommunications, **NETWORK, AND INTERNET** services in
18 conformity with standards and specifications set by international radio,
19 telecommunications, **NETWORK, AND INTERNET** organizations to which the
20 Philippines is a signatory;

21 c) Mandate a fair and reasonable interconnection of facilities of
22 authorized public network operators and other providers of
23 telecommunications, **NETWORK, AND INTERNET** services through
24 appropriate modalities of interconnection and at a reasonable and fair level
25 of charges, which make provision for the cross subsidy to unprofitable local
26 exchange service areas so as to promote telephone [density], **MOBILE**
27 **PHONE, NETWORK, AND BROADBAND DENSITY** and provide the most
28 extensive access to basic telecommunications, **NETWORK, AND INTERNET**
29 services available at affordable rates to the public;

30 xxx

31 e) Promote consumers' welfare by facilitating access to
32 telecommunications, **NETWORK, AND INTERNET SERVICES** whose
33 infrastructure and network must be geared towards the needs of individual

1 and business users, **AND BY DEVELOPING AND IMPLEMENTING STANDARDS,**
2 **PLANS, POLICIES, PROGRAMS, MEASURES, AND MECHANISMS, INCLUDING**
3 **ARBITRATION, QUASI-JUDICIAL, AND PROSECUTORIAL MECHANISMS, TO**
4 **PROTECT THE WELFARE OF CONSUMERS AND USERS OF**
5 **TELECOMMUNICATIONS, NETWORK, AND INTERNET SERVICES;**

6 xxx

7 (b) Article III, Section 6 of the Public Telecommunications Policy Act of the
8 Philippines is hereby amended to read:

9 *Section 6. Responsibilities of and Limitations to Department Powers.* - The
10 Department of [Transportation and Communications (DOTC)] **INFORMATION AND**
11 **COMMUNICATIONS TECHNOLOGY (DICT)** shall not exercise any power which will
12 tend to influence or effect a review or a modification of the Commission's quasi-
13 judicial functions.

14 In coordination with the Commission, however, the Department shall, in
15 accordance with the policies enunciated in this Act, be responsible for:

16 xxx

17 c) the representation and promotion of Philippine interests in
18 international bodies, and the negotiation of the nation's rights and
19 obligations in international [telecommunications] **INFORMATION**
20 **TECHNOLOGY, COMMUNICATIONS, NETWORK, AND INTERNET** matters; and

21 d) the operation of a national consultative forum to facilitate
22 interaction amongst the [telecommunications industries] **INFORMATION,**
23 **COMMUNICATIONS, NETWORK, AND INTERNET INDUSTRIES, USER**
24 **GROUPS,** academic and research institutions in the airing and resolution of
25 important issues in the field of [communications] **TELECOMMUNICATIONS**
26 **AND THE INTERNET.**

27 xxx

28 (c) Article IV of the Public Telecommunications Policy Act of the Philippines is hereby
29 amended to include the following provisions:

30 **SECTION 10A. LOCAL INTERNET SERVICE PROVIDER. – A LOCAL INTERNET**
31 **SERVICE PROVIDER SHALL:**

1 (A) PROVIDE UNIVERSAL INTERNET CONNECTION SERVICE TO ALL
2 SUBSCRIBERS WHO APPLIED FOR SUCH SERVICE, WITHIN A REASONABLE
3 PERIOD AND AT SUCH STANDARDS AS MAY BE PRESCRIBED BY THE
4 COMMISSION AND AT SUCH TARIFF AS TO SUFFICIENTLY GIVE IT A FAIR
5 RETURN ON ITS INVESTMENTS.

6 (B) BE PROTECTED FROM UNCOMPENSATED BYPASS OR
7 OVERLAPPING OPERATIONS OF OTHER TELECOMMUNICATIONS ENTITIES IN
8 NEED OF PHYSICAL LINKS OR CONNECTIONS TO ITS CUSTOMERS IN THE
9 AREA EXCEPT WHEN IT IS UNABLE TO PROVIDE, WITHIN A REASONABLE
10 PERIOD OF TIME AND AT DESIRED STANDARD, THE INTERCONNECTION
11 ARRANGEMENTS REQUIRED BY SUCH ENTITIES.

12 (C) HAVE THE FIRST OPTION TO PROVIDE PUBLIC OR PRIVATE
13 NETWORK ACCESS OR INTERNET ACCESS NODES OR ZONES IN THE AREA
14 COVERED BY ITS NETWORK.

15 (D) BE ENTITLED TO A FAIR AND EQUITABLE REVENUE SHARING
16 ARRANGEMENT WITH THE INTERNET EXCHANGE, INTERNET DATA CENTER,
17 INTERNET GATEWAY FACILITY, OR SUCH OTHER CARRIERS CONNECTED TO
18 ITS BASIC NETWORK.

19 PROVIDED THAT THE SERVICE IT PROVIDES IS SOLELY DEPENDENT ON
20 EXISTING NETWORKS BEING OPERATED AND MAINTAINED BY AT LEAST ONE
21 OTHER TELECOMMUNICATIONS ENTITY, A LOCAL INTERNET SERVICE PROVIDER
22 NEED NOT SECURE A FRANCHISE.

23 A CABLE TV FRANCHISE MAY PROVIDE LOCAL INTERNET CONNECTION,
24 NETWORK, OR DATA TRANSMISSION SERVICES WITHOUT A SEPARATE FRANCHISE;
25 PROVIDED, THAT THE OPERATION OF INTERNET CONNECTION, NETWORK, OR
26 DATA TRANSMISSION SERVICE BY THE CABLE TV FRANCHISE SHALL BE GOVERNED
27 BY THIS ACT AND OTHER RELEVANT LAWS.

28 THE PROVISION OF INTERNET CONNECTION, NETWORK, OR DATA
29 TRANSMISSION SERVICES SHALL BE ALSO BE GOVERNED BY THE PUBLIC SERVICE
30 ACT, AS AMENDED, AND OTHER RELEVANT LAWS GOVERNING UTILITIES.

31 *SECTION 10B. INTERNET EXCHANGE.* – THE NUMBER OF ENTITIES ALLOWED
32 TO PROVIDE INTERNET EXCHANGE SERVICES SHALL NOT BE LIMITED, AND AS A
33 MATTER OF POLICY, WHERE IT IS ECONOMICALLY VIABLE, AT LEAST TWO (2)

1 INTERNET EXCHANGES SHALL BE AUTHORIZED: PROVIDED, HOWEVER, THAT A
2 LOCAL INTERNET SERVICE PROVIDER SHALL NOT BE RESTRICTED FROM OPERATING
3 ITS OWN INTERNET EXCHANGE SERVICE IF ITS VIABILITY IS DEPENDENT THERETO.
4 SUCH INTERNET EXCHANGE SHALL HAVE THE FOLLOWING OBLIGATIONS:

5 (A) IT SHALL INTERCONNECT WITH ALL OTHER INTERNET
6 EXCHANGES IN THE SAME CATEGORY AND WITH ALL LOCAL INTERNET
7 SERVICE PROVIDERS AND OTHER TELECOMMUNICATIONS ENTITIES, UPON
8 APPLICATION AND WITHIN A REASONABLE TIME PERIOD, AND UNDER FAIR
9 AND REASONABLE LEVEL CHARGES, IN ORDER THAT INTERNET AND
10 NETWORK SERVICES ARE MADE POSSIBLE; AND

11 (B) IT SHALL HAVE THE RIGHT TO ESTABLISH AND OPERATE ITS OWN
12 NETWORK FACILITIES THROUGH WHICH INTERNATIONAL NETWORKS OR
13 INTERNATIONAL GATEWAY FACILITIES SHALL BE ABLE TO COURSE THEIR
14 MESSAGES OR SIGNALS.

15 (C) IT SHALL COMPLY WITH INTERNATIONAL AND GENERIC
16 ENGINEERING REQUIREMENTS AND STANDARDS OF OPERATION FOR
17 INTERNET EXCHANGES.

18 *SECTION 10C. INTERNET DATA CENTER.* – THE NUMBER OF ENTITIES
19 ALLOWED TO PROVIDE INTERNET DATA CENTER SERVICES SHALL NOT BE LIMITED,
20 AND AS A MATTER OF POLICY, WHERE IT IS ECONOMICALLY VIABLE, AT LEAST TWO
21 (2) INTERNET DATA CENTERS SHALL BE AUTHORIZED: PROVIDED, HOWEVER, THAT
22 A LOCAL INTERNET SERVICE PROVIDER OR CONTENT PROVIDER SHALL NOT BE
23 RESTRICTED FROM OPERATING ITS OWN INTERNET DATA CENTER IF ITS VIABILITY
24 IS DEPENDENT THERETO. SUCH INTERNET DATA CENTER SHALL HAVE THE
25 FOLLOWING OBLIGATIONS:

26 (A) IT SHALL INTERCONNECT WITH ALL OTHER INTERNET DATA
27 CENTERS IN THE SAME CATEGORY AND WITH ALL LOCAL INTERNET SERVICE
28 PROVIDERS AND OTHER TELECOMMUNICATIONS ENTITIES, UPON
29 APPLICATION AND WITHIN A REASONABLE TIME PERIOD, AND UNDER FAIR
30 AND REASONABLE LEVEL CHARGES, IN ORDER THAT INTERNET AND
31 NETWORK SERVICES ARE MADE POSSIBLE; AND

32 (B) IT SHALL HAVE THE RIGHT TO ESTABLISH AND OPERATE ITS OWN
33 NETWORK FACILITIES THROUGH WHICH INTERNATIONAL NETWORKS OR
34 INTERNATIONAL GATEWAY FACILITIES SHALL BE ABLE TO COURSE THEIR
35 MESSAGES OR SIGNALS.

1 (C) IT SHALL COMPLY WITH INTERNATIONAL AND GENERIC
2 ENGINEERING REQUIREMENTS AND STANDARDS OF OPERATION FOR
3 NETWORK AND DATA CENTERS.

4 **SECTION 10D. INTERNET GATEWAY FACILITY.** – ONLY ENTITIES WHICH WILL
5 PROVIDE INTERNET EXCHANGE SERVICES OR INTERNET DATA CENTER SERVICES,
6 AND CAN DEMONSTRABLY SHOW TECHNICAL AND FINANCIAL CAPABILITY TO
7 INSTALL AND OPERATE AN INTERNATIONAL GATEWAY FACILITY, SHALL BE
8 ALLOWED TO OPERATE AS AN INTERNET GATEWAY FACILITY.

9 THE ENTITY SO ALLOWED SHALL BE REQUIRED TO PRODUCE A FIRM
10 CORRESPONDENT OR INTERCONNECTION RELATIONSHIPS WITH MAJOR OVERSEAS
11 TELECOMMUNICATIONS AUTHORITIES, CARRIERS, OVERSEAS INTERNET
12 GATEWAYS, NETWORKS, AND INTERNET SERVICE PROVIDERS WITHIN ONE (1)
13 YEAR FROM THE GRANT OF THE AUTHORITY.

14 THE INTERNET GATEWAY FACILITY SHALL ALSO COMPLY WITH ITS
15 OBLIGATIONS TO PROVIDE INTERNET EXCHANGE SERVICES IN UNSERVED OR
16 UNDERSERVED AREAS WITHIN THREE (3) YEARS FROM THE GRANT OF THE
17 AUTHORITY AS REQUIRED BY EXISTING REGULATIONS: PROVIDED, HOWEVER,
18 THAT SAID INTERNET GATEWAY FACILITY SHALL BE DEEMED TO HAVE COMPLIED
19 WITH THE SAID OBLIGATION IN THE EVENT IT ALLOWS AN AFFILIATE THEREOF TO
20 ASSUME SUCH OBLIGATION AND WHO COMPLIES THEREWITH.

21 FAILURE TO COMPLY WITH THE ABOVE OBLIGATIONS SHALL BE A CAUSE TO
22 CANCEL ITS AUTHORITY OR PERMIT TO OPERATE AS AN INTERNET GATEWAY
23 FACILITY.

24 **SECTION 10E. CONTENT PROVIDER.** – EXCEPT FOR BUSINESS PERMITS AND
25 OTHER REGULATORY REQUIREMENTS AS PROVIDED FOR BY THE CONSUMER ACT
26 OF THE PHILIPPINES, AS AMENDED, AND OTHER RELEVANT LAWS, AND PROVIDED
27 THAT THE TRANSMISSION OF ITS CONTENT IS SOLELY DEPENDENT ON EXISTING
28 NETWORKS BEING OPERATED AND MAINTAINED BY AT LEAST ONE OTHER
29 TELECOMMUNICATIONS ENTITY, A CONTENT PROVIDER FOR COMMERCIAL OR
30 NON-COMMERCIAL PURPOSES NEED NOT SECURE A FRANCHISE, LICENSE, OR
31 PERMIT TO OPERATE IN THE PHILIPPINES.

32 SUBJECT TO THE NATURE OF THE CONTENT THAT IS PROVIDED BY THE
33 CONTENT PROVIDER FOR COMMERCIAL PURPOSES, LAWS SUCH AS PAGCOR
34 CHARTER, AS AMENDED, THE MTRCB CHARTER, AS AMENDED, AND OTHER

1 **RELEVANT LAWS, SHALL BE DEEMED APPLICABLE TO THE CONTENT PROVIDER.**

2 (d) Article IV, Section 11 of the Public Telecommunications Policy Act of the
3 Philippines is hereby amended to read:

4 *Section 11. Value-added Service Provider.* – Provided that [it does not put up
5 its own network] **THE SERVICE IT PROVIDES IS SOLELY DEPENDENT ON EXISTING**
6 **NETWORKS BEING OPERATED AND MAINTAINED BY AT LEAST ONE OTHER**
7 **TELECOMMUNICATIONS ENTITY**, a VAS provider need not secure a franchise. A VAS
8 provider shall be allowed to competitively offer its services and/or expertise, and
9 lease or rent telecommunications equipment and facilities necessary to provide such
10 specialized services, in the domestic and/or international market in accordance with
11 network compatibility.

12 Telecommunications entities may provide VAS, subject to the additional
13 requirements that:

14 (a) prior approval of the Commission is secured to ensure that such
15 VAS offerings are not cross-subsidized from the proceeds of their utility
16 operations;

17 (b) other providers of VAS are not discriminated against in rates nor
18 denied equitable access to their facilities; and,

19 (c) separate books of accounts are maintained for the VAS.

20 **THE PROVISION OF HIGH-SPEED OR HIGH-VOLUME INTERNET CONNECTION**
21 **OR DATA TRANSMISSION SERVICES AS A SERVICE SEPARATE FROM NORMAL**
22 **INTERNET CONNECTION OR DATA TRANSMISSION SERVICES SHALL NOT BE**
23 **CLASSED AS A VALUE-ADDED SERVICE.**

24 (e) Article V, Section 14 of the Public Telecommunications Policy Act of the
25 Philippines is hereby amended to read:

26 *Section 14. Customer Premises Equipment.* – Telecommunications subscribers
27 **AND INTERNET AND NETWORK USERS** shall be allowed to use within their premises
28 terminal equipment, such as telephone, PABX, facsimile, **SUBSCRIBER**
29 **IDENTIFICATION MODULE (SIM) CARDS**, data, record, message and other special
30 purpose or multi-function telecommunication terminal equipment intended for such
31 connection: Provided, that the equipment is type-approved by the Commission.

1 UNLESS DESIGNED AND MANUFACTURED AS SUCH WITHOUT NEED FOR A
2 SPECIAL REQUEST BY A TELECOMMUNICATIONS ENTITY, NO CUSTOMER PREMISES
3 EQUIPMENT SHALL BE RESTRICTED FROM INTERCONNECTING TO A NETWORK OR
4 TO THE INTERNET, OR INTEROPERABILITY WITH OTHER CUSTOMER PREMISES
5 EQUIPMENT, NETWORK EQUIPMENT, DATA STORAGE EQUIPMENT, OR OTHER
6 DEVICES OR EQUIPMENT THAT MAY BE NORMALLY INTERCONNECTED WITH OR
7 MAY NORMALLY ENJOY INTEROPERABILITY WITH, AS APPLICABLE; PROVIDED,
8 HOWEVER, THAT IN THE COURSE OF NORMAL OPERATIONS SUCH
9 INTERCONNECTION OR INTEROPERABILITY SHALL NOT COMPROMISE DATA OR
10 NETWORK PRIVACY OR SECURITY.

11 (f) Article VII, Section 20 of The Public Telecommunications Policy Act of the
12 Philippines is hereby amended to read:

13 *Section 20. Rights of End-Users.* – The user of telecommunications,
14 **INTERNET, NETWORK, OR DATA TRANSMISSION** service shall have the following
15 basic rights:

16 xxx

17 (C) **RIGHT TO BE GIVEN THE FIRST INTERNET OR NETWORK**
18 **CONNECTION WITHIN TWO (2) MONTHS OF APPLICATION FOR SERVICE,**
19 **AGAINST DEPOSIT; OR WITHIN THREE (3) MONTHS AFTER TARGETED**
20 **COMMENCEMENT OF SERVICE IN THE BARANGAY CONCERNED PER THE**
21 **ORIGINAL SCHEDULE OF SERVICE EXPANSION APPROVED BY THE**
22 **COMMISSION, WHICHEVER DEADLINE COMES LATER;**

23 (d) Regular, timely and accurate billing, courteous and efficient
24 service at utility business offices and by utility company personnel;

25 (E) **TIMELY CORRECTION OF ERRORS IN BILLING AND THE**
26 **IMMEDIATE PROVISION OF REBATES OR REFUNDS BY THE UTILITY**
27 **WITHOUT NEED FOR DEMAND BY THE USER; AND;**

28 (f) Thorough and prompt investigation of, and action upon
29 complaints. The utility shall endeavor to allow complaints [over the
30 telephone] **TO BE RECEIVED BY POST AND OVER MEANS USING**
31 **TELECOMMUNICATIONS FACILITIES OR THE INTERNET, WHICH SHALL**
32 **INCLUDE BUT SHALL NOT BE LIMITED TO VOICE CALLS, SHORT MESSAGE**
33 **SERVICE (SMS) MESSAGES, MULTIMEDIA MESSAGE SERVICE (MMS)**

1 **MESSAGES, OR EMAIL, and shall keep a record of all [written or phoned-in]**
2 **complaints received and the actions taken to address these complaints;**

3 **SUBJECT TO THE FILING OF A FORMAL REQUEST TO THE UTILITY, A USER**
4 **MAY REQUEST THE IMMEDIATE TERMINATION OF SERVICE, WITHOUT THE**
5 **IMPOSITION OF FEES OR PENALTIES, AND WITH THE REFUND OF ANY FEES OR**
6 **CHARGES ALREADY PAID BY THE USER, SHOULD A UTILITY NOT CONSISTENTLY**
7 **COMPLY WITH PRECEDING PARAGRAPHS (A), (D), (E), (F), OR ANY OTHER**
8 **MINIMUM PERFORMANCE STANDARDS SET BY THE COMMISSION.**

9 **SUBJECT TO STANDARDS SET BY THE COMMISSION, REASONABLE FEES OR**
10 **PENALTIES MAY BE IMPOSED BY THE UTILITY, OR MAY BE DEDUCTED FROM ANY**
11 **FEES OR CHARGES ALREADY PAID BY THE USER, SHOULD A USER REQUEST THE**
12 **IMMEDIATE TERMINATION OF SERVICE; PROVIDED THAT:**

13 **(1) THE UTILITY IS ABLE TO SHOW THAT THE REQUEST IS NOT BASED**
14 **ON A NONCOMPLIANCE WITH PRECEDING PARAGRAPHS (A), (D), (E), (F), OR**
15 **ANY OTHER MINIMUM PERFORMANCE STANDARDS SET BY THE**
16 **COMMISSION; OR,**

17 **(2) THE UTILITY HAS EVIDENCE THAT THE NON-COMPLIANCE HAS**
18 **NOT RECURRED, IS NOT RECURRING, NOR WILL RECUR IN THE FUTURE; OR**
19 **THE UTILITY HAS EVIDENCE THAT THE NONCOMPLIANCE WAS DUE TO**
20 **FACTORS BEYOND ITS CONTROL; OR THE UTILITY HAS PROVIDED**
21 **IMMEDIATE REFUND OR REBATE TO THE USER UPON DETECTION OF THE**
22 **NONCOMPLIANCE; OR THE UTILITY HAS EVIDENCE THAT IT HAS EXERTED ITS**
23 **BEST EFFORTS TO RESOLVE THE NONCOMPLIANCE AND RESTORE THE**
24 **SERVICE TO THE LEVEL AGREED BETWEEN THE UTILITY AND THE USER**
25 **WITHIN SEVEN (7) DAYS OF THE REQUEST FOR IMMEDIATE TERMINATION;**
26 **AND THE UTILITY SHALL COMPLY WITH IMMEDIATE TERMINATION OF**
27 **SERVICE, WITHOUT THE IMPOSITION OF FEES OR PENALTIES, AND REFUND**
28 **ANY FEES OR CHARGES ALREADY PAID BY THE USER WITHOUT NEED FOR**
29 **DEMAND SHOULD THE SERVICE NOT BE RESTORED WITHIN THE SEVEN (7)**
30 **DAY PERIOD, WITHIN THREE (3) DAYS AFTER THE TERMINATION OF**
31 **SERVICE.**

32 **SUBJECT TO STANDARDS SET BY THE COMMISSION, PENALTIES MAY BE**
33 **IMPOSED ON A UTILITY THAT IS UNABLE TO COMPLY WITH PRECEDING**
34 **PARAGRAPHS (B) AND (C). THE COMMISSION MAY IMPOSE ADDITIONAL**
35 **PENALTIES IF THE UTILITY DOES NOT REFUND ANY DEPOSITS, FEES, OR CHARGES**
36 **ALREADY PAID BY THE USER WITHOUT NEED FOR DEMAND WITHIN THREE (3)**

1 **DAYS AFTER THE DEADLINE AGREED UPON BETWEEN THE USER AND THE UTILITY.**

2 *Section 18. Quality of Service and Network Fair Use. –*

3 (a) No Internet service provider, Internet exchange, Internet data center, Internet
4 gateway facility, telecommunications entity, or person providing Internet connection,
5 network, or data transmission services shall:

6 (i) Fail to provide a service, or network services on reasonable, and
7 nondiscriminatory terms and conditions such that any person can offer or provide
8 content, applications, or services to or over the network in a manner that is at least
9 equal to the manner in which the provider or its affiliates offer content, applications,
10 and services free of any surcharge on the basis of the content, application, or
11 service;

12 (ii) Refuse to interconnect facilities with other facilities of another provider of
13 network services on reasonable, and nondiscriminatory terms or conditions;

14 (iii) Block, impair, or discriminate against, or to interfere with the ability of
15 any person to use a network service to access, to use, to send, to receive, or to offer
16 lawful content, applications, or services over the Internet;

17 (iv) Impose an additional charge to avoid any conduct that is prohibited by
18 subscription;

19 (v) Prohibit a user from attaching or using a device on the Internet service
20 provider's network that does not physically damage or materially degrade other
21 users' utilization of the network;

22 (vi) Fail to clearly and conspicuously disclose to users, in plain language,
23 accurate information concerning any terms, conditions, or limitations on the
24 network service; or,

25 (vii) Impose a surcharge or other consideration for the prioritization or offer
26 of enhanced quality of service to data or protocol of a particular type, and must
27 provide equal quality of service to all data or protocol of that type regardless of
28 origin or ownership.

29 (b) Nothing in this section shall be construed as to prevent an Internet service
30 provider, Internet exchange, Internet data center, Internet gateway facility,
31 telecommunications entity, or person providing Internet connection, network, or data

1 transmission services from taking reasonable and nondiscriminatory measures:

2 (i) To manage the function of a network on a system-wide basis, provided
3 that such management function does not result in the discrimination between
4 content, application, or services offered by the provider or user;

5 (ii) To give priority to emergency communications;

6 (iii) To prevent a violation of law; or to comply with an order of the court
7 enforcing such law;

8 (iv) To offer consumer protection services such as parental controls, provided
9 users may refuse to enable such services, or opt-out; or,

10 (v) To offer special promotional pricing or other marketing initiatives.

11 (c) An Internet service provider, Internet exchange, Internet data center, Internet
12 gateway facility, telecommunications entity, or person providing Internet connection,
13 network, or data transmission services may provide for different levels of availability,
14 uptime, or other service quality standards set by the National Telecommunications
15 Commission for services using prepaid, postpaid, or other means of payment; *Provided*, that
16 minimum levels of availability, uptime, and other service quality standards set by the
17 Commission shall not be different between services using prepaid, postpaid, or other means
18 of payment.

19 *Section 19. Amendments to the Intellectual Property Code of the Philippines. –*

20 (a) Part IV, Chapter II, Section 172 of the Intellectual Property Code of the Philippines
21 (RA 8293) is hereby amended to read:

22 *Section 172. Literary and Artistic Works. – 172.1. Literary and artistic works,*
23 *hereinafter referred to as "works", are original intellectual creations in the literary*
24 *and artistic domain protected from the moment of their creation and shall include in*
25 *particular:*

26 xxx

27 (n) **CODE, SCRIPTS, COMPUTER PROGRAMS, SOFTWARE**
28 **APPLICATIONS, AND OTHER SIMILAR WORK, WHETHER EXECUTABLE IN**
29 **WHOLE OR AS PART OF ANOTHER CODE, SCRIPT, computer programs,**
30 **SOFTWARE APPLICATION OR OTHER SIMILAR WORK;**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32

xxx

172.2. Works are protected by the sole fact of their creation, irrespective of their mode or form of expression OR PUBLICATION, as well as of their content, quality and purpose.

(b) Part II, Chapter V, Section 177 of the Intellectual Property Code of the Philippines (RA 8293) shall be amended to read:

Section 177. Copyright, [or] COPYLEFT, AND OTHER Economic Rights. – THE ECONOMIC RIGHTS OVER ORIGINAL AND DERIVATIVE LITERARY AND ARTISTIC WORKS SHALL BE ANY OF THE FOLLOWING:

177.1 COPYRIGHT – SUBJECT TO THE PROVISIONS OF CHAPTER VIII, ECONOMIC RIGHTS UNDER THIS SECTION SHALL CONSIST OF THE EXCLUSIVE RIGHT TO CARRY OUT, AUTHORIZE OR PREVENT THE FOLLOWING ACTS:

xxx

177.2. COPYLEFT – IS THE EXERCISE OF ECONOMIC RIGHTS OVER ORIGINAL AND DERIVATIVE WORKS, INCLUDING FREE AND OPEN-SOURCE SOFTWARE, WHERE THE AUTHOR IRREVOCABLY ASSIGNS TO THE PUBLIC, EITHER PARTIALLY OR FULLY, ONE OR SEVERAL RIGHTS IN COMBINATION, THE RIGHT TO USE, MODIFY, EXTEND, OR REDISTRIBUTE THE ORIGINAL WORK. UNDER COPYLEFT, ANY AND ALL WORKS DERIVED FROM THE ORIGINAL WORK SHALL BE COVERED BY THE SAME LICENSE AS THE ORIGINAL WORK. DECLARATION OF A COPYLEFT LICENSE SHALL BE SUFFICIENT IF A STATEMENT OF THE APPLICABLE COPYLEFT LICENSE IS STIPULATED ON A COPY OF THE WORK AS PUBLISHED.

177.3 FREE OR PUBLIC – IS THE EXERCISE OF ECONOMIC RIGHTS OVER ORIGINAL AND DERIVATIVE WORKS WHERE THE AUTHOR IRREVOCABLY ASSIGNS TO THE PUBLIC ALL THE RIGHTS TO USE, MODIFY, EXTEND, OR REDISTRIBUTE THE ORIGINAL WORK WITHOUT ANY RESTRICTIONS, OR WHERE THE AUTHOR IRREVOCABLY DECLARES THE WORK TO BE PUBLIC DOMAIN UNDER SECTIONS 175 AND 176 OF THIS CODE. THE REDISTRIBUTION OF ANY MODIFIED OR DERIVATIVE WORK SHALL NOT BE REQUIRED TO ADOPT FREE OR PUBLIC RIGHT. ADOPTION OR DECLARATION OF THIS RIGHT SHALL BE SUFFICIENT IF A STATEMENT TO THE

1 EFFECT IS STIPULATED ON A COPY OF THE WORK AS PUBLISHED.

2 177.4 EXCEPT WITH RESPECT TO ECONOMIC RIGHTS UNDER
3 COPYLEFT, THE AUTHOR OR COPYRIGHT OWNER SHALL HAVE THE OPTION
4 TO DECLARE THE TYPE OF LICENSE OR ECONOMIC RIGHTS THAT MAY BE
5 EXERCISED BY THE PUBLIC IN RELATION TO THE WORK; PROVIDED THAT,
6 FAILURE OF THE AUTHOR OR COPYRIGHT OWNER TO MAKE SUCH
7 DECLARATION SHALL BE CONSTRUED AS CLAIM OF ECONOMIC RIGHTS
8 UNDER SECTION 177.1.

9 (c) Part II, Chapter VII, Section 180 of the Intellectual Property Code of the
10 Philippines (RA 8293) shall be amended to read:

11 *Section 180. Rights of Assignee of Copyright.* – 180.1. The **ECONOMIC RIGHTS**
12 **UNDER SECTION 177.1** may be assigned in whole or in part. Within the scope of the
13 assignment, the assignee is entitled to all the rights and remedies which the assignor
14 or licensor had with respect to the copyright.

15 xxx

16 180.3. The submission of a literary, photographic or artistic work to a
17 newspaper, magazine or periodical for publication, shall constitute only a license to
18 make a single publication unless a greater right is expressly granted. **IN THE CASE OF**
19 **POSTING TO A WEBSITE OR AN ONLINE VERSION OF A NEWSPAPER, MAGAZINE,**
20 **OR PERIODICAL, ENABLING ACCESS TO THE WHOLE OR PORTION OF THE WORK VIA**
21 **AUTOMATIC CONTENT SYNDICATION OR SEARCH RESULTS SHALL NOT CONSTITUTE**
22 **VIOLATION OF THE LICENSE UNLESS THE CONTRARY IS EXPRESSLY PROVIDED IN A**
23 **WRITTEN AGREEMENT BETWEEN COPYRIGHT OWNER AND**
24 **PUBLISHER/HOST/SERVICE PROVIDER.** If two (2) or more persons jointly own a
25 copyright or any part thereof, neither of the owners shall be entitled to grant
26 licenses without the prior written consent of the other owner or owners.

27 xxx

28 (d) Part II, Chapter VII, Section 182 of the Intellectual Property Code of the
29 Philippines (RA 8293) shall be amended to read:

30 *Section 182. Filing of Assignment or License OF COPYRIGHT.* – An assignment
31 or exclusive license may be filed in duplicate with the National Library upon payment
32 of the prescribed fee for registration in books and records kept for the purpose.
33 Upon recording, a copy of the instrument shall be returned to the sender with a

1 notation of the fact of record. Notice of the record shall be published in the IPO
2 Gazette.

3 xxx

4 (e) Part II, Chapter VII, Section 187 of the Intellectual Property Code of the
5 Philippines (RA 8293) shall be amended to read:

6 *Section 187. Reproduction of Published Work.* – 187.1. Subject to the
7 provisions of Section 177 [and subject to the provisions] in relation to the provision
8 of Subsection 187.2, the private reproduction of a published work in a single copy,
9 where the reproduction is made by a natural person exclusively for research and
10 private study, shall be permitted, without the authorization of the owner of
11 copyright in the work.

12 2. The permission granted under Subsection 187.1 shall not extend to the
13 reproduction of:

14 xxx

15 (c) A compilation of **RAW data, HAVING NOT UNDERGONE DATA AND**
16 **INFORMATION PROCESSING**, and other materials;

17 xxx

18 **(E) THE CONTENTS OF A WEBSITE, IF SUCH DOWNLOADING IS FOR**
19 **THE PURPOSE OF CREATING A BACK-UP COPY FOR ARCHIVAL PURPOSES, OR**
20 **EXCLUSIVELY TO TEMPORARILY FACILITATE THE EXECUTION OF COMPUTER**
21 **APPLICATIONS, SUCH AS BUT NOT LIMITED TO SEARCH ENGINES, OR**
22 **EXCLUSIVELY TO TEMPORARILY FACILITATE THE OPERATION OF THE**
23 **INTERNET OR NETWORKS, SUCH AS BUT NOT LIMITED TO CACHE COPIES,**
24 **OR EXCLUSIVELY FOR PURPOSES OF STATISTICAL OR PERFORMANCE**
25 **ANALYSIS; and,**

26 xxx

27 (f) Part II, Chapter IX, Section 192 of the Intellectual Property Code of the Philippines
28 (RA 8293) shall be amended to read:

29 *Section 192. Notice of [Copyright] APPLICABLE ECONOMIC RIGHTS.* – Each
30 copy of a work published or offered for sale may contain a notice bearing the name

1 of the copyright owner, and the year of its first publication, and, in copies produced
2 after the creator's death, the year of such death. **IN CASE OF FAILURE OF THE**
3 **AUTHOR OR COPYRIGHT OWNER TO INDICATE THE LICENSE APPLICABLE FOR THE**
4 **WORK, IT SHALL BE PRESUMED THAT THE COPYRIGHT OWNER ADOPTED**
5 **COPYRIGHT UNLESS INTENT TO THE CONTRARY IS PROVEN.**

6 *Section 20. Content Fair Use. –*

7 (a) Subject to the provisions of the Intellectual Property Code of the Philippines (RA
8 8293), as amended, and this Act and other relevant laws, the viewing of online content on
9 any computer, device, or equipment shall be considered fair use.

10 (b) Subject to the provisions of the Intellectual Property Code of the Philippines, as
11 amended, this Act, and other relevant laws, the viewing, use, editing, decompiling, or
12 modification, of downloaded or otherwise offline content on any computer, device, or
13 equipment shall be considered fair use; *Provided*, that the derivative content resulting from
14 editing, decompiling, or modification shall be subject to the provisions of the Intellectual
15 Property Code of the Philippines (RA 8293), as amended, this Act, and other relevant laws
16 governing derivative content.

17 (c) It shall be presumed that any person who shall upload to, download from, edit,
18 modify, or otherwise use content on the Internet or telecommunications networks shall
19 have done so with full knowledge of the nature of the intellectual property protections
20 applicable to the content.

21 *Section 21. Amendments to the E-Commerce Act. –* Subject to the provisions of this Act,
22 paragraphs (a) and (b) of Section 33 of the Electronic Commerce Act of 2000 (RA 8792) are
23 hereby repealed.

24 *Section 22. Amendments to the Data Privacy Act. –*

25 (a) Subject to the provisions of this Act, Section 7 of the Data Privacy Act of 2012 (RA
26 10173) is hereby amended in part to read:

27 *Section 7. Functions of the National DATA Privacy Commission. –* To
28 administer and implement the provisions of this Act, and to monitor and ensure
29 compliance of the country with international standards set for data protection, there
30 is hereby created an independent body to be known as the National DATA Privacy
31 Commission, which shall have the following functions:...

32 (b) Subsequent mentions of "National Privacy Commission" are hereby amended to

1 be consistent with the amendment above.

2 (c) Subject to the provisions of this Act, Sections 29, 31, and 32 of the Data Privacy
3 Act of 2012 are repealed.

4 (d) Subject to the provisions of this Act, Section 6 of the Data Privacy Act of 2012 is
5 amended to include the provisions on extraterritoriality as provided for by Section 67 of this
6 Act.

7 *Section 23. Repeal of the Cybercrime Prevention Act.* – The Cybercrime Prevention Act of
8 2012 (RA 10175) is repealed in its entirety.

9 **Part 5. Cybercrimes and Other Prohibited Acts.**

10 *Section 24. Network Sabotage.* –

11 (a) *Direct network sabotage.* – It shall be unlawful for any person to cause or attempt
12 to cause the stoppage or degradation of Internet or network operations of another person,
13 through electronic means such as denial of service (DoS) attacks or distributed denial of
14 service (DDoS) attacks, through physical destruction of devices, equipment, physical plant,
15 or telecommunications cables including cable TV transmission lines and other transmission
16 media, or through other means, except if the stoppage or degradation has been done in the
17 normal course of work or business by a person authorized to stop, modify, or otherwise
18 control network operations of the other person.

19 (b) *Indirect network sabotage.* – It shall be unlawful for any person to install, infect,
20 implant, or otherwise put in a device, equipment, network, or physical plant any means of
21 performing stoppage, degradation, or modification of Internet or network operations, or
22 data or information processing, such as but not limited to bots, or to interconnect, establish,
23 or otherwise create a network of software, devices, equipment, or physical plants with the
24 means of performing stoppage, degradation, or modification of Internet or network
25 operations, or data or information processing, such as but not limited to botnets, except if
26 the installation or interconnection has been done in the normal course of work or business
27 by a person authorized to stop, modify, or otherwise control network operations or data or
28 information processing of the network.

29 (c) *Criminal negligence not presumed in unintentional network sabotage.* – Except
30 upon a final ruling from the courts, issued following due notice and hearing, criminal
31 negligence shall not be presumed to be the cause of the unintentional stoppage or
32 degradation of Internet or network operations by a person authorized to stop, modify, or
33 otherwise control network operations, or by accident, unforeseen occurrences, or acts of

1 God.

2 *Section 25. Failure to Provide Reasonable Security for Data and Networks. –*

3 (a) *Failure to provide security.* – It shall be unlawful for any Internet service provider,
4 telecommunications entity, or other such person providing Internet or data services to
5 intentionally or unintentionally fail to provide appropriate levels of security for data,
6 networks, storage media where data is stored, equipment through which networks are run
7 or maintained, or the physical plant where the data or network equipment is housed.

8 (b) *Negligent failure to provide security.* – Negligence resulting to acts in violation of
9 the Data Privacy Act of 2012 (RA 10175) using a device, network equipment, or physical
10 plant connected to the Internet, public networks, private networks, or telecommunications
11 facilities shall constitute a violation of the preceding paragraph, without prejudice to
12 prosecution under the Data Privacy Act of 2012 (RA 10175).

13 (c) *Negligent failure to provide security presumed to be the result of criminal*
14 *negligence.* – The unintentional failure for any Internet service provider,
15 telecommunications entity, or other such person providing Internet or data services to
16 provide appropriate levels of security for data, networks, storage media where data is
17 stored, equipment through which networks are run or maintained, or the physical plant
18 where the data or network equipment is housed shall be presumed to be the result of
19 criminal negligence, except upon a final ruling from the courts, issued following due notice
20 and hearing.

21 *Section 26. Violation of Data Privacy. –*

22 (a) *Unauthorized access.* – It shall be unlawful for any person to intentionally access
23 data, networks, storage media where data is stored, equipment through which networks are
24 run or maintained, the physical plant where the data or network equipment is housed,
25 without authority granted by the Internet service provider, telecommunications entity, or
26 other such person providing Internet or data services having possession or control of the
27 data or network, or to intentionally access intellectual property published on the Internet or
28 on other networks without the consent of the person having ownership, possession, or
29 control of the intellectual property, or without legal grounds, even if access is performed
30 without malice.

31 (b) *Unauthorized modification.* – It shall be unlawful for any person to intentionally
32 modify data, networks, storage media where data is stored, equipment through which
33 networks are run or maintained, the physical plant where the data or network equipment is
34 housed, without authority granted by the Internet service provider, telecommunications

1 entity, or other such person providing Internet or data services having possession or control
2 of the data or network, or to intentionally modify intellectual property published on the
3 Internet or on other networks without the consent of the person having ownership,
4 possession, or control of the intellectual property, or without legal grounds, even if the
5 modification is performed without malice.

6 (c) *Unauthorized authorization or granting of privileges.* – It shall be unlawful for any
7 person to intentionally provide a third party authorization or privileges to access or modify
8 data, networks, storage media where data is stored, equipment through which networks are
9 run or maintained, the physical plant where the data or network equipment is housed,
10 without authority granted by the Internet service provider, telecommunications entity, or
11 other such person providing Internet or data services having possession or control of the
12 data or network, or to intentionally provide a third party authorization to access or modify
13 intellectual property published on the Internet or on other networks without the consent of
14 the person having ownership, possession, or control of the intellectual property, or without
15 legal grounds, even if the authorization to access or perform modifications was granted
16 without malice.

17 (d) *Unauthorized disclosure.* – It shall be unlawful for any authorized person to
18 intentionally disclose or cause the disclosure to a third party or to the public any private
19 data being transmitted through the Internet or through public networks, or any data being
20 transmitted through private networks, without legal grounds, even if the disclosure was
21 done without malice.

22 (e) *Violation of Data Privacy Act through ICT.* – It shall be unlawful to perform acts in
23 violation of the Data Privacy Act of 2012 (RA 10175) using a device, network equipment, or
24 physical plant connected to the Internet, public networks, private networks, or
25 telecommunications facilities.

26 *Section 27. Violation of Data Security.* –

27 (a) *Hacking.* – It shall be unlawful for any unauthorized person to intentionally access
28 or to provide a third party with access to, or to hack or aid or abet a third party to hack into,
29 data, networks, storage media where data is stored, equipment through which networks are
30 run or maintained, the physical plant where the data or network equipment is housed. The
31 unauthorized access or unauthorized act of providing a third party with access to, or the
32 hacking into, data, networks, storage media where data is stored, equipment through which
33 networks are run or maintained, the physical plant where the data or network equipment is
34 housed shall be presumed to be malicious.

35 (b) *Cracking.* – It shall be unlawful for any unauthorized person to intentionally

1 modify or to crack data, networks, storage media where data is stored, equipment through
2 which networks are run or maintained, the physical plant where the data or network
3 equipment is housed, or for any unauthorized person to intentionally modify intellectual
4 property published on the Internet or on other networks. The unauthorized modification or
5 cracking of data, networks, storage media where data is stored, equipment through which
6 networks are run or maintained, the physical plant where the data or network equipment is
7 housed, or unauthorized modification of intellectual property published on the Internet or
8 on other networks, shall be presumed to be malicious.

9 (c) *Phishing.* –

10 (i) It shall be unlawful for any unauthorized person to intentionally acquire or
11 to cause the unauthorized acquisition, or identity or data theft, or phishing of private
12 data, security information, or data or information used as proof of identity of
13 another person. The unauthorized acquisition or causing to acquire, or identity or
14 data theft, or phishing of private data, security information, or data or information
15 used as proof of identity of another person shall be presumed to be malicious.

16 (ii) Malicious disclosure of unwarranted or false information relative to any
17 personal information or personal sensitive information obtained by him or her as
18 defined by Section 31 of the Data Privacy Act of 2012 (RA 10175) shall constitute
19 phishing.

20 (d) *Violation of Data Privacy Act in series or combination with hacking, cracking, or*
21 *phishing.* – It shall be unlawful to perform acts in violation of the Data Privacy Act of 2012
22 (RA 10175) using a device, network equipment, or physical plant connected to the Internet,
23 public networks, private networks, or telecommunications facilities performed in series or
24 combination with acts prohibited by the preceding paragraphs.

25 *Section 28. Illegal and Arbitrary Seizure.* –

26 (a) *Illegal Seizure.* – It shall be unlawful for any person to seize data, information, or
27 contents of a device, storage medium, network equipment, or physical plant, or to seize any
28 device, storage medium, network equipment, or physical plant connected to the Internet or
29 to telecommunications networks of another person without his consent, or to gain
30 possession or control of the intellectual property published on the Internet or on public
31 networks of another person without his consent, except upon a final ruling from the courts,
32 issued following due notice and hearing.

33 (b) *Aiding and Abetting Illegal Seizure.* – It shall be unlawful for any person to aid or
34 abet the seizure of data, information, or contents of a device, storage medium, network

1 equipment, or physical plant, or to seize any device, storage medium, network equipment,
2 or physical plant connected to the Internet or to telecommunications networks of another
3 person without his consent, or to gain possession or control of the intellectual property
4 published on the Internet or on public networks of another person without his consent,
5 except upon a final ruling from the courts, issued following due notice and hearing, allowing
6 the person to perform such seizure, possession, or control.

7 (c) *Arbitrary Seizure.* – It shall be unlawful for any public officer or employee to seize
8 data, information, or contents of a device, storage medium, network equipment, or physical
9 plant, or to seize any device, storage medium, network equipment, or physical plant
10 connected to the Internet or to telecommunications networks, or to gain possession or
11 control of intellectual property published on the Internet or on public networks, without
12 legal grounds.

13 (d) *Instigating Arbitrary Seizure.* – It shall be unlawful for any person to instruct a
14 public officer or employee to perform the seizure of data, information, or contents of a
15 device, storage medium, network equipment, or physical plant, or to seize any device,
16 storage medium, network equipment, or physical plant connected to the Internet or to
17 telecommunications networks of another person without his consent, or to gain possession
18 or control of the intellectual property published on the Internet or on public networks of
19 another person without his consent, except upon a final ruling from the courts, issued
20 following due notice and hearing, providing the person with authority to perform such
21 seizure, possession, or control and delegate the same to a public officer or employee with
22 the authority to perform such seizure, possession, or control.

23 *Section 29. Infringement of Intellectual Property Rights.* –

24 (a) *Copyright infringement.* –

25 (i) Subject to the Intellectual Property Code of the Philippines and the laws
26 governing fair use, it shall be unlawful for any person to publish or reproduce on the
27 Internet, in part or in whole, any content that he does not have any economic rights
28 over, or does not acknowledge and comply with the terms of copyright or license
29 governing the intellectual property rights enjoyed by the content being published or
30 reproduced, or falsely claims having intellectual property rights over the content he
31 does not own.

32 (ii) Non-attribution or plagiarism of copyleft content shall constitute
33 infringement.

34 (iii) Non-attribution or plagiarism of free license or public domain content

1 shall constitute infringement, but shall not be subject to damages.

2 (iv) Subject to the Intellectual Property Code of the Philippines and the laws
3 governing fair use, it shall be unlawful for any person to reverse-engineer any whole
4 or part of any computer program, software, code, or script, whether or not
5 executable, that is the subject of a copyright, and that he does not have any
6 property rights over, or does not acknowledge and comply with the terms of
7 copyright or license governing the intellectual property rights enjoyed by the
8 computer program being reverse-engineered.

9 (b) *Piracy.* – Subject to the Intellectual Property Code of the Philippines, it shall be
10 unlawful for any person to publish and reproduce, with intent to profit, on the Internet or
11 on or through information and communications technologies, in part or in whole, any
12 content, or computer program, software, code, or script, whether or not executable, that he
13 does not have any property rights over.

14 (c) *Cybersquatting.* – Subject to the Intellectual Property Code of the Philippines and
15 other relevant laws, and the Uniform Domain Name Dispute Resolution Policy of the
16 Internet Corporation for Assigned Names and Numbers (ICANN) or any policy of ICANN or
17 successor-in-interest superseding it, it shall be unlawful for any person to register or
18 otherwise acquire, in bad faith to profit or to damage, a domain name that is:

19 (i) Similar, identical, or confusingly similar to an existing trademark registered
20 with the appropriate government agency at the time of the domain name
21 registration; or

22 (ii) Identical or in any way similar with the name of a person other than the
23 registrant, in case of a personal name.

24 (d) *Unreasonable restriction of device privileges.* – Subject to Section 6 of this Act, it
25 shall be unlawful for any person engaged in the wholesale or retail of devices or equipment
26 to, by physical, electronic, or any other means, provide unreasonable restrictions on a
27 device or equipment.

28 *Section 30. Fraud via ICT.* – It shall be unlawful for any person who knowingly by means of a
29 device, equipment, or physical plant connected to the Internet, to telecommunications
30 networks, a network of a government agency, the government network, a private network
31 or any protected computer or device, or in connivance with a third party with access to the
32 same, shall use the Internet, telecommunications networks, private networks, or
33 government networks for the purpose of deceiving or defrauding another of money, goods,
34 or property, or to do the same by or through exceeding authorized access.

1 *Section 31. ICT-Enabled Prostitution and ICT-Enabled Trafficking in Persons. –*

2 (a) *ICT-Enabled Prostitution.* – It shall be unlawful for any person who, by means of a
3 device, equipment, or physical plant connected to the Internet or to telecommunications
4 networks, or in connivance with a third party with access to the same, shall use the Internet
5 or telecommunications networks for the purpose of enabling the exchange of money or
6 consideration for services of a sexual or lascivious nature, or facilitating the performance of
7 such services; *Provided*, the services shall be performed by one or more unwilling third-
8 party adults under threat or duress.

9 (b) *ICT-Enabled Trafficking in Persons. –*

10 (i) The performance of acts prohibited by Section 5 of R.A. No. 9208, or the
11 “Anti-Trafficking in Persons Act of 2003,” as amended, by means of a device, storage
12 medium, network equipment, or physical plant connected to the Internet or to
13 telecommunications networks shall be deemed unlawful.

14 (ii) The commission of acts prohibited by the Anti-Trafficking in Persons Act of
15 2003, as amended, through or using devices, equipment, or physical plants
16 connected to the Internet or to telecommunications networks shall be penalized by
17 the applicable provisions of the Anti-Trafficking in Persons Act of 2003, as amended.

18 (iii) Section 5 (c) of the Anti-Trafficking in Persons Act of 2003 shall be
19 amended to read:

20 *Section 5. Acts that Promote Trafficking in Persons. –* The following
21 acts which promote or facilitate trafficking in persons, shall be unlawful:

22 xxx

23 (c) To advertise, publish, print, broadcast or distribute, or
24 cause the advertisement, publication, printing, broadcasting or
25 distribution by any means, including the use of information **AND**
26 **COMMUNICATIONS** technology and the Internet, of any brochure,
27 flyer, or any propaganda material that promotes trafficking in
28 persons, **OR TO KNOWINGLY, WILLFULLY AND INTENTIONALLY**
29 **PROVIDE DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED**
30 **TO THE INTERNET OR TO TELECOMMUNICATIONS NETWORKS, WITH**
31 **THE PRIMARY PURPOSE OF PROMOTING TRAFFICKING IN PERSONS;**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32

Section 32. ICT-Enabled Child Prostitution and ICT-Enabled Child Trafficking. –

(a) ICT-Enabled Child Prostitution. -

(i) The performance of acts prohibited by Sections 5 and 7 of R.A. No. 7610, or the "Special Protection of Children Against Abuse, Exploitation and Discrimination Act," as amended, by means of a device, storage medium, network equipment, or physical plant connected to the Internet or to telecommunications networks shall be deemed unlawful.

(ii) Section 5, paragraphs (a) 2 and (c) of the "Special Protection of Children Against Abuse, Exploitation and Discrimination Act" shall be amended to read:

Section 5. Child Prostitution and Other Sexual Abuse. –

xxx

(2) Inducing a person to be a client of a child prostitute by means of written or oral advertisements or other similar means; **OR TO KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED TO THE INTERNET OR TO TELECOMMUNICATIONS NETWORKS WITH THE PRIMARY PURPOSE OF INDUCING A PERSON TO BE A CLIENT OF A CHILD PROSTITUTE OR THROUGH THE CONNIVANCE WITH A THIRD PARTY WITH ACCESS TO THE SAME INDUCE A PERSON TO BE A CLIENT OF A CHILD PROSTITUTE;**

xxx

(c) Those who derive profit or advantage therefrom, whether as manager or owner of the establishment where the prostitution takes place, or of the sauna, disco, bar, resort, place of entertainment or establishment serving as a cover or which engages in prostitution in addition to the activity for which the license has been issued to said establishment; **OR THOSE WHO DERIVE PROFIT OR ADVANTAGE THEREFROM, WHETHER AS AUTHOR, ADMINISTRATOR, OR AUTHORIZED USER OF THE DEVICE, EQUIPMENT, NETWORK, PHYSICAL PLANT, OR WEBSITE CONNECTED TO THE INTERNET OR TO**

1 TELECOMMUNICATIONS NETWORKS CREATED OR ESTABLISHED
2 WITH THE PURPOSE OF INDUCING A PERSON TO ENGAGE IN CHILD
3 PROSTITUTION.

4 xxx

5 (b) *ICT-Enabled Child Trafficking.* –

6 (i) Section 7 of the “Special Protection of Children Against Abuse, Exploitation
7 and Discrimination Act” shall be amended to read:

8 Section 7. *Child Trafficking.* – Any person who shall engage in trading
9 and dealing with children including, but not limited to, the act of buying and
10 selling of a child for money, or for any other consideration, or barter, **OR TO**
11 **KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE DEVICES,**
12 **EQUIPMENT, OR PHYSICAL PLANTS CONNECTED TO THE INTERNET OR TO**
13 **TELECOMMUNICATIONS NETWORKS, OR THROUGH THE CONNIVANCE**
14 **WITH A THIRD PARTY WITH ACCESS TO THE SAME, FOR THE PRIMARY**
15 **PURPOSE OF SUCH TRADING AND DEALING WITH CHILDREN,** shall suffer the
16 penalty of *reclusion temporal* to *reclusion perpetua*. The penalty shall be
17 imposed in its maximum period when the victim is under twelve (12) years of
18 age.

19 (ii) The commission of acts prohibited by the “Special Protection of Children
20 Against Abuse, Exploitation and Discrimination Act,” as amended, through or using
21 devices, equipment, or physical plants connected to the Internet or to
22 telecommunications networks shall be penalized by the applicable provisions of the
23 “Special Protection of Children Against Abuse, Exploitation and Discrimination Act,”
24 as amended.

25 *Section 33. Internet Libel, Hate Speech, Child Pornography, and Other Expression Inimical to*
26 *the Public Interest.* –

27 (a) *Internet libel.* –

28 (i) Internet libel is a public and malicious expression tending to cause the
29 dishonor, discredit, or contempt of a natural or juridical person, or to blacken the
30 memory of one who is dead, made on the Internet or on public networks.

31 (ii) *Malice as an essential element of internet libel.* – Internet libel shall not lie
32 if malice or intent to injure is not present.

1 (iii) *Positive identification of the subject as an essential element of internet*
2 *libel.* – Internet libel shall not lie if the public and malicious expression does not
3 explicitly identify the person who is the subject of the expression, except if the
4 content of the expression is sufficient for positive and unequivocal identification of
5 the subject of the expression.

6 (iv) *Truth as a defense.* – Internet libel shall not lie if the content of the
7 expression is proven to be true, or if the expression is made on the basis of
8 published reports presumed to be true, or if the content is intended to be humorous
9 or satirical in nature, except if the content has been adjudged as unlawful or
10 offensive in nature in accordance with existing jurisprudence.

11 (v) *Exceptions to internet libel.* – The following acts shall not constitute
12 internet libel:

13 (1) Expressions of protest against the government, or against foreign
14 governments;

15 (2) Expressions of dissatisfaction with the government, its agencies or
16 instrumentalities, or its officials or agents, or with those of foreign
17 governments;

18 (3) Expressions of dissatisfaction with non-government organizations,
19 unions, associations, political parties, religious groups, and public figures;

20 (4) Expressions of dissatisfaction with the products or services of
21 commercial entities;

22 (5) Expressions of dissatisfaction with commercial entities, or their
23 officers or agents, as related to the products or services that the commercial
24 entities provide;

25 (6) Expressions of a commercial entity that are designed to discredit
26 the products or services of a competitor, even if the competitor is explicitly
27 identified;

28 (7) An expression made with the intention of remaining private
29 between persons able to access or view the expression, even if the
30 expression is later released to the public; and,

1 (8) A fair and true report, made in good faith, without any comments
2 or remarks, of any judicial, legislative or other official proceedings, or of any
3 statement, report or speech delivered in said proceedings, or of any other act
4 performed by public officers in the exercise of their functions, or of any
5 matter of public interest.

6 (b) *Internet hate speech.* –

7 (i) Internet hate speech is a public and malicious expression calling for the
8 commission of illegal acts on an entire class of persons, a reasonably broad section
9 thereof, or a person belonging to such a class, based on gender, sexual orientation,
10 religious belief or affiliation, political belief or affiliation, ethnic or regional affiliation,
11 citizenship, or nationality, made on the Internet or on public networks.

12 (ii) *Call for the commission of illegal acts as an essential element for internet*
13 *hate speech.* – Internet hate speech shall not lie if the expression does not call for
14 the commission of illegal acts on the person or class of persons that, when they are
15 done, shall cause actual criminal harm to the person or class of persons, under
16 existing law.

17 (iii) *Imminent lawless danger as an essential element for internet hate speech.*
18 – Internet hate speech shall not lie if the expression does not call for the commission
19 of illegal acts posing an immediate lawless danger to the public or to the person who
20 is the object of the expression.

21 (c) *Internet child pornography.* –

22 (i) The performance of acts prohibited by Sections 4 and 5 of R.A. No. 9775,
23 or the “Anti-Child Pornography Act of 2009,” as amended, by means of a device,
24 storage medium, network equipment, or physical plant connected to the Internet or
25 to telecommunications networks shall be deemed unlawful.

26 (ii) The commission of acts prohibited by the Anti-Child Pornography Act of
27 2009, as amended, through or using devices, equipment, or physical plants
28 connected to the Internet or to telecommunications networks shall be penalized by
29 the applicable provisions of the Anti-Child Pornography Act of 2009, as amended.

30 (iii) Sections 4 (e) and (f) of the Anti-Child Pornography Act of 2009 shall be
31 amended to read:

1 (e) To knowingly, willfully and intentionally provide a venue for the
2 commission of prohibited acts as, but not limited to, dens, private rooms,
3 cubicles, cinemas, houses or in establishments purporting to be a legitimate
4 business; **OR TO KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE**
5 **DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED TO THE INTERNET**
6 **OR TO TELECOMMUNICATIONS NETWORKS FOR THE PRIMARY PURPOSE OF**
7 **PUBLICATION, OFFERING, PRODUCTION, SELLING, DISTRIBUTION,**
8 **BROADCASTING, EXPORT, OR IMPORTATION OF CHILD PORNOGRAPHY;**

9 (f) For film distributors, theaters, **INTERNET SERVICE PROVIDERS**, and
10 telecommunication companies, by themselves or in cooperation with other
11 entities, to distribute any form of child pornography;

12 xxx

13 (d) *Internet child abuse.* –

14 (i) The performance of acts prohibited by Section 9 of the Special Protection
15 of Children Against Abuse, Exploitation and Discrimination Act, as amended, by
16 means of a device, storage medium, network equipment, or physical plant
17 connected to the Internet or to telecommunications networks shall be deemed
18 unlawful.

19 (ii) The commission of acts prohibited by the Special Protection of Children
20 Against Abuse, Exploitation and Discrimination Act, as amended, through or using
21 devices, equipment, or physical plants connected to the Internet or to
22 telecommunications networks shall be penalized by the applicable provisions of the
23 Special Protection of Children Against Abuse, Exploitation and Discrimination Act, as
24 amended.

25 (iii) Section 9 of the Special Protection of Children Against Abuse, Exploitation
26 and Discrimination Act shall be amended to read:

27 *Section 9. Obscene Publications and Indecent Shows.* – Any person
28 who shall hire, employ, use, persuade, induce or coerce a child to perform in
29 obscene exhibitions and indecent shows, whether live, in video, or through
30 the Internet or telecommunications networks, or model in obscene
31 publications or pornographic materials or to sell or distribute or **CAUSE THE**
32 **PUBLICATION IN THE INTERNET OR THROUGH TELECOMMUNICATIONS**
33 **NETWORKS** the said materials shall suffer the penalty of *prision mayor* in its

1 medium period.

2 xxx

3 (e) *Expression inimical to the public interest.* –

4 (i) Except upon a final ruling from the courts, issued following due notice or
5 hearing, no expression made on the Internet or on public networks that is not
6 defined in this section shall be deemed unlawful and inimical to the public interest.

7 (ii) *Imminent lawless danger as an essential element of expression inimical to*
8 *public interest.* – No expression shall be deemed inimical to the public interest if the
9 expression does not call for the commission of illegal acts posing an immediate
10 lawless danger to the public.

11 *Section 34. Sabotage of Critical Networks and Infrastructure, Acts of Cyberterrorism, and*
12 *Cyberespionage.* –

13 (a) *Sabotage of critical networks and infrastructure.* – The commission of acts
14 prohibited by Section 42 (Network Sabotage), Section 44 (Violation of Data Privacy), Section
15 45 (Violation of Data Security), and Section 46 (Illegal and Arbitrary Seizure of ICT), shall be
16 penalized one degree higher; *Provided*, the offense was committed against critical data,
17 network, Internet, or telecommunications infrastructure, whether publicly or privately
18 owned.

19 (b) *Cyberterrorism.* –

20 (i) The performance of acts prohibited by Sections 3, 4, 5, and 6 of the Human
21 Security Act of 2007 (RA9732) as amended, and Sections 4, 5, 6, and 7 of the
22 Terrorism Financing Prevention and Suppression Act of 2012 (RA 10168), or the by
23 means of a device, storage medium, network equipment, or physical plant
24 connected to the Internet or to telecommunications networks shall be deemed
25 unlawful.

26 (ii) The commission of acts prohibited by the Human Security Act of 2007, as
27 amended, through or using devices, equipment, or physical plants connected to the
28 Internet or to telecommunications networks shall be penalized by the applicable
29 provisions of the Human Security Act of 2007, as amended.

30 (iii) Section 3 of the Human Security Act of 2007 shall be amended to read:

1 *Section 3. Terrorism.* – Any person who commits an act punishable
 2 under any of the following provisions of the Revised Penal Code:

3 xxx

4 6. Presidential Decree No. 1866, as amended (Decree
 5 Codifying the Laws on Illegal and Unlawful Possession, Manufacture,
 6 Dealing in, Acquisition or Disposition of Firearms, Ammunitions or
 7 Explosives); and,

8 **7. SECTION 25 (NETWORK SABOTAGE), SECTION 27**
 9 **(VIOLATION OF DATA PRIVACY), AND SECTION 28 (VIOLATION OF**
 10 **DATA SECURITY) OF THE MAGNA CARTA FOR PHILIPPINE INTERNET**
 11 **FREEDOM COMMITTED AGAINST CRITICAL DATA, NETWORK,**
 12 **INTERNET, OR TELECOMMUNICATIONS INFRASTRUCTURE, WHETHER**
 13 **PUBLICLY OR PRIVATELY OWNED,**

14 xxx

15 (c) *ICT-Enabled Financing of Terrorism.* –

16 (i) The commission of acts prohibited by the Terrorism Financing Prevention
 17 and Suppression Act of 2012, as amended, through or using devices, equipment, or
 18 physical plants connected to the Internet or to telecommunications networks shall
 19 be penalized by the applicable provisions of the Terrorism Financing Prevention and
 20 Suppression Act of 2012, as amended.

21 (ii) Section 4 of the Terrorism Financing Prevention and Suppression Act of
 22 2012 shall be amended to read:

23 *Section 4. Financing of Terrorism.* –

24 xxx

25 Any person who organizes or directs others to commit financing of
 26 terrorism under the immediately preceding paragraph shall likewise be guilty
 27 of an offense and shall suffer the same penalty as herein prescribed.

28 **ANY PERSON WHO, BY MEANS OF A DEVICE, STORAGE MEDIUM,**
 29 **NETWORK EQUIPMENT, OR PHYSICAL PLANT CONNECTED TO THE INTERNET**
 30 **OR TO TELECOMMUNICATIONS NETWORKS, OR IN CONNIVANCE WITH A**

1 THIRD PARTY WITH ACCESS TO THE SAME, SHALL KNOWINGLY, WILLFULLY,
2 AND INTENTIONALLY FACILITATE THE ORGANIZATION OR DIRECTION OF
3 OTHERS TO COMMIT THE FINANCING OF TERRORISM UNDER THE
4 PRECEDING PARAGRAPHS SHALL LIKEWISE BE GUILTY OF AN OFFENSE AND
5 SHALL SUFFER THE SAME PENALTY AS HEREIN PRESCRIBED.

6 XXX

7 (d) *Cyber-espionage*. – Article 117 of the Revised Penal Code shall be amended to
8 read:

9 *Art. 117. Espionage*. — The penalty of *prision correccional* shall be inflicted
10 upon any person who:

11 XXX

12 2. WITHOUT AUTHORITY THEREFOR, OR EXCEEDING THE AUTHORITY
13 GRANTED BY THE STATE, AND BY MEANS OF A DEVICE, EQUIPMENT, OR
14 PHYSICAL PLANT CONNECTED TO THE INTERNET, TO
15 TELECOMMUNICATIONS NETWORKS, A NETWORK OF THE STATE, A
16 PRIVATE NETWORK, OR ANY PROTECTED DEVICE, COMPUTER, SYSTEM, OR
17 NETWORK, OR IN CONNIVANCE WITH A THIRD PARTY WITH ACCESS TO THE
18 SAME, SHALL USE THE INTERNET, TELECOMMUNICATIONS NETWORKS,
19 NETWORKS OF THE STATE, OR PRIVATE NETWORKS TO OBTAIN ANY DATA
20 OR INFORMATION OF A CONFIDENTIAL NATURE RELATIVE TO THE DEFENSE
21 OF THE PHILIPPINES OR ANY DATA OR INFORMATION CLASSIFIED BY LAW
22 AS STATE SECRETS; OR

23 3. Being in possession, by reason of the public office he holds, of the
24 articles, data, or information referred to in the preceding paragraphs,
25 discloses their contents to a representative of a foreign nation OR HOSTILE
26 NON-STATE ACTOR.

27 XXX

28 **Part 6. National Cybersecurity, Cyberdefense, Counter-Cyberterrorism, and**
29 **Counter-Cyberespionage.**

30 *Section 35. Cyberwarfare and National Defense*. –

31 (a) It shall be unlawful for any person, or military or civilian agency, or

1 instrumentality of the State to initiate a cyberattack against any foreign nation, except in
2 the event of a declaration of a state of war with the foreign nation.

3 (b) Subject to the Geneva Convention, the Hague Convention, the United Nations
4 Convention on Certain Conventional Weapons, other international treaties and conventions
5 governing the conduct of warfare, Philippine law, and on authority by the President of the
6 Philippines or by his designated officers, an authorized person or military agency may
7 engage in cyberdefense in defense of the Filipino people, territory, economy, and vital
8 infrastructure in the event of a cyberattack by a foreign nation, enemy violent non-state
9 actor, insurgent group, or terrorist organization.

10 (c) Any person who initiates an unauthorized and unlawful cyberattack against a
11 foreign nation shall be prosecuted under Commonwealth Act 408, as amended, or
12 applicable military law, without prejudice to criminal and civil prosecution.

13 *Section 36. National Cybersecurity and Protection of Government Information and*
14 *Communications Technology Infrastructure. –*

15 (a) The Secretary of National Defense shall assist the President in the protection and
16 conduct of the national cybersecurity, and the conduct of cyberdefense and the protection
17 of national government information and communications technology infrastructure.

18 (b) The Armed Forces of the Philippines shall be tasked with ensuring the physical
19 and network security of critical government and military information and communications
20 infrastructure. The Philippine National Police shall assist private and public owners,
21 operators, and maintainers in ensuring the physical and network security of critical
22 information and communications infrastructure.

23 (c) Local government units shall be responsible for cyberdefense within their
24 jurisdiction. The Secretary of the Interior and Local Government, with the assistance of the
25 Secretary of National Defense, shall be assist local government units in the development of
26 plans, policies, programs, measures, and mechanisms for cybersecurity and cyberdefense of
27 at the local government level and the protection of local government systems, networks,
28 and information and communications technology infrastructure.

29 (d) When national interest and public safety so require, and subject to the approval
30 of Congress in a special session called for the purpose, the President may be granted the
31 authority to direct the cyberdefense and cybersecurity of local government units; *Provided,*
32 that Congress may not grant such authority for a period longer than 90 days.

33 *Section 37. Amendments to the AFP Modernization Act. – Section 5 of the AFP*

1 Modernization Act (RA 7898) shall be amended to include:

2 *Section 5. Development of AFP Capabilities.* – The AFP modernization program shall
3 be geared towards the development of the following defense capabilities:

4 xxx

5 (d) Development of cyberdefense capability. – [The modernization of the AFP
6 further requires the development of the general headquarters capabilities for
7 command, control, communications, and information systems network.] **THE
8 PHILIPPINE AIR FORCE (PAF), BEING THE COUNTRY'S FIRST LINE OF EXTERNAL
9 DEFENSE, SHALL DEVELOP ITS CYBERDEFENSE CAPABILITY. THE CYBERDEFENSE
10 CAPABILITY SHALL ENABLE THE AFP TO:**

11 **(1) DETECT, IDENTIFY, INTERCEPT AND ENGAGE, IF NECESSARY, ANY
12 ATTEMPTED OR ACTUAL PENETRATION OR CYBERATTACK OF PHILIPPINE
13 GOVERNMENT INFORMATION AND COMMUNICATIONS TECHNOLOGY
14 INFRASTRUCTURE, AS WELL AS CRITICAL INFORMATION AND
15 COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE WITHIN PHILIPPINE
16 JURISDICTION;**

17 **(2) PROVIDE CYBERDEFENSE SUPPORT TO PHILIPPINE ARMED
18 FORCES AND POLICE FORCES, AND;**

19 **(3) PROVIDE, AND IF PRACTICABLE, INVENT OR INNOVATE,
20 THROUGH FILIPINO SKILLS AND TECHNOLOGY, ITS OWN REQUIREMENTS
21 FOR NATIONAL CYBERDEFENSE.**

22 **(E) DEVELOPMENT OF CYBERINTELLIGENCE CAPABILITY. – THE
23 INTELLIGENCE SERVICE OF THE ARMED FORCES OF THE PHILIPPINES (ISAFP) OR ITS
24 SUCCESSOR SERVICE, SHALL DEVELOP ITS CYBERINTELLIGENCE CAPABILITY. THE
25 CYBERINTELLIGENCE CAPABILITY SHALL ENABLE THE AFP TO:**

26 **(1) DETECT ANY THREAT AGAINST PHILIPPINE GOVERNMENT
27 INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE,
28 AS WELL AS CRITICAL INFORMATION AND COMMUNICATIONS
29 TECHNOLOGY INFRASTRUCTURE WITHIN PHILIPPINE JURISDICTION, AND
30 IDENTIFY THE SOURCE OF THE THREAT, WHETHER HOSTILE NATION-STATES,
31 NON-STATE ACTORS, CYBERTERRORISTS, OR CRIMINALS;**

32 **(2) PROVIDE CYBERINTELLIGENCE SUPPORT TO PHILIPPINE ARMED**

1 **FORCES AND POLICE FORCES, AND;**

2 **(3) PROVIDE, AND IF PRACTICABLE, INVENT OR INNOVATE,**
3 **THROUGH FILIPINO SKILLS AND TECHNOLOGY, ITS OWN REQUIREMENTS**
4 **FOR NATIONAL CYBERINTELLIGENCE.**

5 **(F) DEVELOPMENT OF GOVERNMENT AND MILITARY INFORMATION AND**
6 **COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE HARDENED AGAINST**
7 **CYBERATTACK. — THE COMMUNICATIONS, ELECTRONICS AND INFORMATION**
8 **SYSTEM SERVICE, ARMED FORCES OF THE PHILIPPINES (CEISSAFP) OR ITS**
9 **SUCCESSOR SERVICE, SHALL CONTINUALLY ENSURE THAT GOVERNMENT AND**
10 **MILITARY INFORMATION AND COMMUNICATIONS TECHNOLOGY**
11 **INFRASTRUCTURE ARE HARDENED AGAINST CYBERATTACK.**

12 xxx

13 *Section 38. Counter-Cyberterrorism. —*

14 (a) The Philippine National Police, supported by applicable military, law
15 enforcement, and government services, offices, and agencies, shall be the lead law
16 enforcement agency responsible for plans, policies, programs, measures, and mechanisms
17 to detect, identify, and prevent cyberterrorist attacks on Philippine government information
18 and communications technology infrastructure, as well as publicly- and privately-owned
19 information and communications technology infrastructure within Philippine jurisdiction,
20 and the detection, identification, pursuit, apprehension, and the gathering of evidence
21 leading to the conviction of persons committing cyberterrorism.

22 (b) The National Bureau of Investigation, supported by applicable military, law
23 enforcement, and government services, offices, and agencies, shall be the lead law
24 enforcement agency responsible for plans, policies, programs, measures, and mechanisms
25 to detect, identify, and prevent transnational cyberterrorist attacks on Philippine
26 government information and communications technology infrastructure, as well as publicly-
27 and privately-owned information and communications technology infrastructure within
28 Philippine jurisdiction

29 (c) Subject to the provisions of an existing treaty to which the Philippines is a
30 signatory and to any contrary provision of any law of preferential application, and subject to
31 the concurrence of the Secretary of Justice and the Secretary of Foreign Affairs, the Director
32 of the National Bureau of Investigation may cooperate with or request the cooperation of
33 foreign or international law enforcement agencies in the detection, identification, pursuit,
34 apprehension, and the gathering of evidence leading to the conviction of persons who,

1 although physically outside the territorial limits of the Philippines, have committed or are
2 attempting to commit acts of cyberterrorism within Philippine jurisdiction.

3 *Section 39. Counter-Cyberespionage. –*

4 (a) The National Intelligence Coordinating Agency, supported by applicable military,
5 law enforcement, and government services, offices, and agencies, shall be the lead agency
6 responsible for plans, policies, programs, measures, and mechanisms to detect, identify, and
7 prevent cyberespionage attempts and incidents.

8 (b) The National Bureau of Investigation, supported by applicable military, law
9 enforcement, and government services, offices, and agencies, shall be the lead agency
10 responsible for detection, identification, pursuit, apprehension, and the gathering of
11 evidence leading to the conviction of persons committing cyberespionage.

12 **Part 7. Penalties.**

13 *Section 40. Applicability of the Revised Penal Code and other special laws. –* The provisions
14 of Book I of the Revised Penal Code shall apply suppletorily to the provisions of this Act,
15 whenever applicable.

16 The provisions of special laws shall apply as provided for by this Act.

17 *Section 41. Penalties For Specific Violations of The Magna Carta for Philippine Internet*
18 *Freedom. –* The following penalties shall be imposed for specific violations of this Act:

19 (a) Violation of Section 42 (a) (Direct network sabotage) – Shall be punished with
20 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
21 pesos (PhP500,000.00) or both.

22 (b) Violation of Section 42 (b) (Indirect network sabotage) - Shall be punished with
23 imprisonment of *prision correccional* in its medium period or a fine of not more than three
24 hundred thousand pesos (PhP300,000.00) or both.

25 (c) Violation of Section 43 (a) (Failure to provide security) - Shall be punished with
26 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
27 pesos (PhP500,000.00) or both.

28 (d) Violation of Section 43 (b) (Negligent failure to provide security) - Shall be
29 punished with imprisonment of *prision correccional* or a fine of not more than Five hundred
30 thousand pesos (PhP500,000.00) or both.

1 (e) Violation of Section 44 (a) (Unauthorized access) – Shall be punished with
2 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
3 hundred thousand pesos (Php500,000.00) but not more than Two million pesos
4 (Php2,000,000.00).

5 (f) Violation of Section 44 (b) (Unauthorized modification) - Shall be punished with
6 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
7 hundred thousand pesos (Php500,000.00) but not more than Two million pesos
8 (Php2,000,000.00).

9 (g) Violation of Section 44 (c) (Unauthorized granting of privileges) - Shall be
10 punished with imprisonment ranging from one (1) year to three (3) years and a fine of not
11 less than Five hundred thousand pesos (Php500,000.00) but not more than Two million
12 pesos (Php2,000,000.00).

13 (h) Violation of Section 44 (d) (Unauthorized disclosure) - imprisonment ranging from
14 three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos
15 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

16 (i) Violations of the Section 44 (e) (Violation of Data Privacy Act through ICT) –

17 (i) Violation of Section 25 (a) of the Data Privacy Act (Unauthorized
18 Processing of Personal Information) through ICT – imprisonment ranging from one
19 (1) year to three (3) years and a fine of not less than Five hundred thousand pesos
20 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

21 (ii) Violation of Section 25 (b) of the Data Privacy Act (Unauthorized
22 Processing of Sensitive Personal Information) through ICT – imprisonment ranging
23 from three (3) years to six (6) years and a fine of not less than Five hundred
24 thousand pesos (Php500,000.00) but not more than Four million pesos
25 (Php4,000,000.00).

26 (iii) Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal
27 Information Due to Negligence) through ICT – imprisonment ranging from one (1)
28 year to three (3) years and a fine of not less than Five hundred thousand pesos
29 (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

30 (iv) Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
31 Personal Information Due to Negligence) through ICT – imprisonment ranging from
32 three (3) years to six (6) years and a fine of not less than Five hundred thousand

1 pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

2 (v) Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of
3 Personal Information) through ICT – imprisonment ranging from six (6) months to
4 two (2) years and a fine of not less than One hundred thousand pesos
5 (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00).

6 (vi) Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of
7 Sensitive Personal Information) through ICT – imprisonment ranging from one (1)
8 year to three (3) years and a fine of not less than One hundred thousand pesos
9 (Php100,000.00) but not more than One million pesos (Php1,000,000.00).

10 (vii) Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal
11 Information for Unauthorized Purposes) through ICT – imprisonment ranging from
12 one (1) year and six (6) months to five (5) years and a fine of not less than Five
13 hundred thousand pesos (Php500,000.00) but not more than One million pesos
14 (Php1,000,000.00).

15 (viii) Violation of Section 28 (b) of the Data Privacy Act (Processing of
16 Sensitive Personal Information for Unauthorized Purposes) through ICT –
17 imprisonment ranging from two (2) years to seven (7) years and a fine of not less
18 than Five hundred thousand pesos (Php500,000.00) but not more than Two million
19 pesos (Php2,000,000.00).

20 (ix) Violation of Section 30 of the Data Privacy Act (Concealment of Security
21 Breaches Involving Sensitive Personal Information) through ICT – imprisonment of
22 one (1) year and six (6) months to five (5) years and a fine of not less than Five
23 hundred thousand pesos (Php500,000.00) but not more than One million pesos
24 (Php1,000,000.00).

25 (x) Violation of Section 33 of the Data Privacy Act (Combination or Series of
26 Acts) through ICT – imprisonment ranging from three (3) years to six (6) years and a
27 fine of not less than One million pesos (Php1,000,000.00) but not more than Five
28 million pesos (Php5,000,000.00).

29 (j) Violation of Section 45 (a) (Hacking) – imprisonment ranging from one (1) year to
30 three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but
31 not more than Two million pesos (Php2,000,000.00).

32 (k) Violation of Section 45 (b) (Cracking) – imprisonment ranging from one (1) year to
33 three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but

1 not more than Two million pesos (Php2,000,000.00).

2 (l) Violation of Section 45 (c) (Phishing) – imprisonment ranging from one (1) year
3 and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos
4 (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

5 (m) Violation of Section 45 (d) (Violation of Data Privacy Act with hacking, cracking,
6 or phishing) –

7 (i) Violation of Section 25 (a) of the Data Privacy Act (Unauthorized
8 Processing of Personal Information) with hacking, cracking, or phishing – shall be
9 penalized by imprisonment ranging from one (1) year to three (3) years and a fine of
10 not less than Five hundred thousand pesos (Php500,000.00) but not more than Two
11 million pesos (Php2,000,000.00).

12 (ii) Violation of Section 25 (b) of the Data Privacy Act (Unauthorized
13 Processing of Sensitive Personal Information) with hacking, cracking, or phishing –
14 shall be penalized by imprisonment ranging from three (3) years to six (6) years and
15 a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more
16 than Four million pesos (Php4,000,000.00).

17 (iii) Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal
18 Information Due to Negligence) with hacking, cracking, or phishing – shall be
19 penalized by imprisonment ranging from one (1) year to three (3) years and a fine of
20 not less than Five hundred thousand pesos (Php500,000.00) but not more than Two
21 million pesos (Php2,000,000.00).

22 (iv) Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
23 Personal Information Due to Negligence) with hacking, cracking, or phishing – shall
24 be penalized by imprisonment ranging from three (3) years to six (6) years and a fine
25 of not less than Five hundred thousand pesos (Php500,000.00) but not more than
26 Four million pesos (Php4,000,000.00).

27 (v) Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of
28 Personal Information) with hacking, cracking, or phishing – shall be penalized by
29 imprisonment ranging from six (6) months to two (2) years and a fine of not less than
30 One hundred thousand pesos (Php100,000.00) but not more than Five hundred
31 thousand pesos (Php500,000.00).

32 (vi) Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of
33 Sensitive Personal Information) with hacking, cracking, or phishing – shall be

1 penalized by imprisonment ranging from one (1) year to three (3) years and a fine of
2 not less than One hundred thousand pesos (Php100,000.00) but not more than One
3 million pesos (Php1,000,000.00).

4 (vii) Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal
5 Information for Unauthorized Purposes) with hacking, cracking, or phishing – shall be
6 penalized by imprisonment ranging from one (1) year and six (6) months to five (5)
7 years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but
8 not more than One million pesos (Php1,000,000.00).

9 (viii) Violation of Section 28 (b) of the Data Privacy Act (Processing of
10 Sensitive Personal Information for Unauthorized Purposes) with hacking, cracking, or
11 phishing – shall be penalized by imprisonment ranging from two (2) years to seven
12 (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00)
13 but not more than Two million pesos (Php2,000,000.00).

14 (ix) Violation of Section 30 of the Data Privacy Act (Concealment of Security
15 Breaches Involving Sensitive Personal Information) with hacking, cracking, or
16 phishing – Shall be penalized by imprisonment of one (1) year and six (6) months to
17 five (5) years and a fine of not less than Five hundred thousand pesos
18 (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

19 (x) Violation of Section 33 of the Data Privacy Act (Combination or Series of
20 Acts) with hacking, cracking, or phishing – Shall be penalized by imprisonment
21 ranging from three (3) years to six (6) years and a fine of not less than One million
22 pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

23 (n) Violation of Section 46 (a) (Illegal seizure of ICT) – shall be punished with
24 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
25 pesos (PhP500,000.00) or both.

26 (o) Violation of Section 46 (b) (Aiding and abetting illegal seizure of ICT) – shall be
27 punished with imprisonment of *prision correccional* in its minimum period or a fine of not
28 more than Four hundred thousand pesos (PhP400,000.00) or both.

29 (p) Violation of Section 46 (c) (Arbitrary seizure of ICT) – Shall be punished with
30 imprisonment of *prision correccional* in its maximum period or a fine of not more than Five
31 hundred thousand pesos (PhP500,000.00) or both.

32 (q) Violation of Section 46 (d) (Instigating arbitrary seizure of ICT) – shall be punished
33 with imprisonment of *prision correccional* or a fine of not more than Five hundred thousand

1 pesos (PhP500,000.00) or both.

2 (r) Violation of Section 47 (a) (i) (Copyright infringement) – any person infringing a
3 copyright shall be liable to pay to the copyright proprietor or his assigns or heirs such actual
4 damages, including legal costs and other expenses, as he may have incurred due to the
5 infringement as well as the profits the infringer may have made due to such infringement,
6 and in proving profits the plaintiff shall be required to prove sales only and the defendant
7 shall be required to prove every element of cost which he claims, or, in lieu of actual
8 damages and profits, such damages which to the court shall appear to be just and shall not
9 be regarded as penalty.

10 (s) Violation of Section 47 (a) (ii) (Plagiarism of copyleft) – The same penalty for a
11 violation of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this
12 Section.

13 (t) Violation of Section 47 (a) (iii) (Plagiarism of public domain content) – While this
14 constitutes infringement, it shall not be subject to the payment of damages or to any other
15 penalty.

16 (u) Violation of Section 47 (a) (iv) (Reverse engineering) – The same penalty for a
17 violation of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this
18 Section.

19 (v) Violation of Section 47 (b) (Piracy through ICT) – The same penalty for a violation
20 of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this Section.

21 (w) Violation of Section 47 (c) (Cybersquatting) – The same penalty for a violation of
22 Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this Section.

23 (x) Violation of Section 47 (d) (Unreasonable restriction of device privileges) – shall
24 be punished with a fine of not less than one hundred thousand pesos (PhP 100,000.00) or
25 more than two million pesos (PhP 2,000,000.00).

26 (y) Violation of Section 48 (Fraud via ICT) – shall be punished with imprisonment of
27 *prision correccional* or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to
28 a maximum amount that is double the amount of damage incurred, whichever is higher, or
29 both imprisonment and fine.

30 (z) Violation of Section 49 (a) (ICT-enabled prostitution) – shall be punished with
31 imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos
32 (PhP200,000.00) up to a maximum amount of Five hundred thousand pesos

1 (PhP500,000.00), or both.

2 (aa) Violation of Section 49 (b) (ICT-enabled trafficking in persons) –

3 (i) Violation of Section 4 of the Anti-Trafficking in Persons Act of 2003
4 through ICT – penalty of imprisonment of twenty (20) years and a fine of not less
5 than One million pesos (P1,000,000.00) but not more than Two million pesos
6 (P2,000,000.00).

7 (ii) Violation of Section 5 of the Anti-Trafficking in Persons Act of 2003
8 through ICT – imprisonment of fifteen (15) years and a fine of not less than Five
9 hundred thousand pesos (P500,000.00) but not more than One million pesos
10 (P1,000,000.00).

11 (iii) Violation of Section 6 of the Anti-Trafficking in Persons Act of 2003
12 through ICT – life imprisonment and a fine of not less than Two million pesos
13 (P2,000,000.00) but not more than Five million pesos (P5,000,000.00).

14 (iv) Violation of Section 7 of the Anti-Trafficking in Persons Act of 2003
15 through ICT – imprisonment of six (6) years and a fine of not less than Five hundred
16 thousand pesos (P500,000.00) but not more than One million pesos (P1,000,000.00).

17 (ab) Violation of Section 50 (a) (ICT-enabled child prostitution) – Violation of Section
18 5 of the Special Protection of Children Against Abuse, Exploitation and Discrimination Act
19 through ICT – *reclusion temporal* in its medium period to *reclusion perpetua*.

20 (ac) Violation of Section 50 (b) (ICT-enabled child trafficking) – Violation of Section 7
21 of the Special Protection of Children Against Abuse, Exploitation and Discrimination Act
22 through ICT – *reclusion temporal* to *reclusion perpetua*. The penalty shall be imposed in its
23 maximum period when the victim is under twelve (12) years of age.

24 (ad) Violation of Section 51 (a) (Internet libel) – This shall only give rise to civil
25 liability and the amount shall be commensurate to the damages suffered.

26 (ae) Violation of Section 51 (b) (Internet hate speech) – This shall only give rise to
27 civil liability and the amount shall be commensurate to the damages suffered.

28 (af) Violation of Section 51 (c) (Internet child pornography) – Violation of the Anti-
29 Child Pornography Act through ICT – Shall be punished according to the provisions of
30 Section 15 of the Anti-Child Pornography Act of 2009 (RA 9775)

1 (ag) Violation of Section 51 (d) (Internet child abuse) – Violation of Section 9 of the
2 Special Protection of Children Against Abuse, Exploitation and Discrimination Act through
3 ICT - Shall be punished with imprisonment of *prision mayor* in its medium period. If the child
4 used as a performer, subject or seller/ distributor is below twelve (12) years of age, the
5 penalty shall be imposed in its maximum period.

6 (ah) Violation of Section 51 (e) (Internet expression inimical to the public interest) –
7 This shall only give rise to civil liability and the amount shall be commensurate to the
8 damages caused by the Internet expression.

9 (ai) Violation of Section 52 (b) (Cyberterrorism) – The commission of acts prohibited
10 by the Human Security Act of 2007, as amended, through or using devices, equipment, or
11 physical plants connected to the Internet or to telecommunications networks shall be
12 penalized by the applicable provisions of the Human Security Act of 2007, as amended.

13 (aj) Violation of Section 52 (c) (ICT-enabled financing of terrorism) – The commission
14 of acts prohibited by the Terrorism Financing Prevention and Suppression Act of 2012, as
15 amended, through or using devices, equipment, or physical plants connected to the Internet
16 or to telecommunications networks shall be penalized by the applicable provisions of the
17 Terrorism Financing Prevention and Suppression Act of 2012, as amended.

18 (ak) Violation of Section 52 (d) (Cyberespionage) – The commission of acts prohibited
19 by Article 117 of the Revised Penal Code, as amended, through or using devices, equipment,
20 or physical plants connected to the Internet or to telecommunications networks shall be
21 penalized by the applicable provisions of the Revised Penal Code, as amended.

22 *Section 42. Penalties for Violations of the Magna Carta for Philippine Internet Freedom*
23 *Affecting Critical Networks and Infrastructure.* – As prescribed by Section 52 (a) of this Act, a
24 penalty one degree higher shall be imposed on the specific violations of the Magna Carta for
25 Philippine Internet Freedom if committed against critical networks or information and
26 communications technology infrastructure.

27 *Section 43. Penalties for Other Violations of The Magna Carta for Philippine Internet*
28 *Freedom.* – A fine of not more than Five hundred thousand pesos (PhP 500,000.00) shall be
29 imposed for a violation of other sections of the law not covered by the preceding sections.

30 *Section 44. Penalties for Violations of The Magna Carta for Philippine Internet Freedom*
31 *Committed by a Public Official or Employee.* –

32 (a) Except as explicitly provided by the preceding sections, the next higher penalty
33 shall be imposed for a violation or negligence resulting in the violation of this Act if the

1 violation or negligence resulting in the violation is committed by a public official or
2 employee in connection with his duties.

3 (b) If the penalty imposed for the act or negligence resulting in the violation of this
4 Act is civil liability or civil liability and a fine, then an additional penalty of a fine of not less
5 Two hundred thousand pesos (PhP 200,000.00) but not more than Five hundred thousand
6 pesos (PhP 500,000.00) shall be imposed on the public official or employee.

7 *Section 45. Liability Under the Data Privacy Act, the Intellectual Property Code, the Optical*
8 *Media Act, the Anti-Child Pornography Act of 2009, the Special Protection of Children*
9 *Against Abuse, Exploitation and Discrimination Act, the Revised Penal Code, and Other Laws.*
10 -

11 (a) A prosecution under this act shall bar any further prosecution of the act as a
12 violation of any provision of the Data Privacy Act, the Intellectual Property Code, the Optical
13 Media Act, the Anti-Child Pornography Act of 2009, the Anti-Trafficking in Persons Act, and
14 other special laws, except:

15 (i) if the act was performed through the use of a device, equipment, or
16 physical plant connected to the Internet or to telecommunications networks, or in
17 connivance with a third party with access to the same; and,

18 (ii) if the act could not have been performed through the use the said device,
19 equipment, or physical plant connected to the Internet or to telecommunications
20 networks, or the said third party with access to the same, and; c) if the act is part of
21 a series of or combination with other unlawful acts, these acts being performed
22 without the use of a device, equipment, or physical plant connected to the Internet
23 or to telecommunications networks, or in connivance with a third party with access
24 to the same.

25 (b) A prosecution under this act shall bar any further prosecution of the act as a
26 violation of the Revised Penal Code and other special laws, except:

27 (i) if the act was performed through the use of a device, equipment, or
28 physical plant connected to the Internet or to telecommunications networks, or in
29 connivance with a third party with access to the same;

30 (ii) if the violation could not have been performed through the use the said
31 device, equipment, or physical plant connected to the Internet or to
32 telecommunications networks, or the said third party with access to the same;

1 (iii) if the act involves the transmission of data through the Internet or
2 telecommunications networks; and

3 (iv) if the act is part of a series of or combination with other unlawful acts,
4 these acts being performed without the use of a device, equipment, or physical plant
5 connected to the Internet or to telecommunications networks, or in connivance with
6 a third party with access to the same.

7 *Section 46. Competent Law Enforcement Agencies. –*

8 (a) *Department of Justice (DOJ).* – The Department of Justice may create an Office of
9 Cybercrime, which shall be designated as the central authority in the enforcement of this
10 Act, and all matters related to international mutual assistance and extradition, as provided
11 for by this Act.

12 (b) *National Bureau of Investigation (NBI).* – The National Bureau of Investigation
13 may create a Cybercrime Division, which shall be responsible for matters related to
14 enforcement of this Act. It shall cooperate with the division responsible for matters related
15 with transnational crime, other divisions, and other government agencies in the
16 enforcement of this Act.

17 (c) *Philippine National Police (PNP).* – The Criminal Investigation and Detection
18 Group (CIDG) of the Philippine National Police may create a Cybercrime Office, which shall
19 be responsible for matters related to enforcement of this Act. The PNP shall, within the
20 extent practicable, establish cybercrime desks in police stations, and shall cooperate with
21 other government agencies in the enforcement of this Act.

22 *Section 47. Cybercrime Courts. –*

23 (a) *Designation of Cybercrime Courts and Promulgation of Procedural Rules.* – The
24 Supreme Court shall designate the court or courts, manned by judges of competence,
25 integrity, probity and independence in the practice of law, and competent in matters
26 related to the Internet and information and communications technology, that will hear and
27 resolve cases brought under this Act and shall promulgate the rules of pleading, practice
28 and procedure to govern the proceedings brought under this Act.

29 (b) *Qualifications of the Presiding Judges of cybercrime courts.* – No person shall be
30 appointed a Presiding Judge of the Cybercrime Court unless he:

31 (i) is a natural-born citizen of the Philippines;

1 (ii) is at least thirty-five (35) years of age;

2 (iii) has been engaged in the practice of law in the Philippines for at least ten
3 (10) years, or has held a public office in the Philippines requiring admission to the
4 practice of law as an indispensable requisite; and,

5 (iv) has an academic or professional background in information and
6 communications technology, computer science, or engineering; or has proven a high
7 degree of competence in the use of the Internet and information and
8 communications technology.

9 Court personnel of the Cybercrime Court shall undergo training and must have the
10 experience and demonstrated ability in dealing with cybercrime cases and other cases
11 related to the Internet and information and communications technology.

12 *Section 48. Jurisdiction of Cybercrime Courts. –*

13 (a) *Exclusive original jurisdiction* – The Cybercrime Court shall have exclusive original
14 jurisdiction over violations of this Act and over cases involving the Internet and information
15 and communications technology.

16 (b) *Suit filed at the residence of the accused for criminal violations of the Magna*
17 *Carta for Philippine Internet Freedom.* – Except in cases that are extraterritorial, foreign,
18 international, and transnational in nature, all suits related to criminal violations of this Act
19 shall be filed at the cybercrime court having jurisdiction over the residence of the accused.

20 (c) *Suit filed at the cybercrime court agreed upon by the parties for civil violations of*
21 *the Magna Carta for Philippine Internet Freedom.* – Except in cases that are extraterritorial,
22 foreign, international, and transnational in nature, all suits related to civil violations of this
23 Act shall be filed at the cybercrime court agreed upon by the parties. Should the parties be
24 unable to reach an agreement, the Court of Appeals shall determine the cybercrime court
25 that shall have jurisdiction over the case.

26 *Section 49. Extraterritorial application of the Magna Carta for Philippine Internet Freedom. –*
27 Subject to the provision of an existing treaty of which the Philippines is a State Party, and to
28 any contrary provision of any law of preferential application, the provisions of this Act shall
29 apply:

30 (a) to individual persons who, although physically outside the territorial limits of the
31 Philippines, commit, conspire or plot to commit any of the crimes defined and punished in
32 this Act inside the territorial limits of the Philippines;

1 (b) to individual persons who, although physically outside the territorial limits of the
2 Philippines, commit any of the said crimes on board a Philippine ship or aircraft;

3 (c) to individual persons who commit any of said crimes within any embassy,
4 consulate, or diplomatic premises belonging to or occupied by the Philippine government in
5 an official capacity;

6 (d) to individual persons who, although physically outside the territorial limits of the
7 Philippines, commit said crimes against Philippine citizens or persons of Philippine descent,
8 where their citizenship or ethnicity was a factor in the commission of the crime; and,

9 (e) to individual persons who, although physically outside the territorial limits of the
10 Philippines, commit said crimes directly against the Philippine government or critical
11 information and communications technology infrastructure in the Philippines.

12 **Part 8. Implementing Rules and Regulations.**

13 *Section 50. General Implementing Rules and Regulations for the Implementation of the*
14 *Magna Carta for Philippine Internet Freedom. –*

15 (a) The Secretary of Information and Communication Technology, the Commissioner
16 of the National Telecommunications Commission, the Commissioner of the National Data
17 Privacy Commission, and the Chief of the Telecommunications Office, or their duly
18 authorized and appointed delegates, an appointee from the academe or the business
19 sector, and an appointee from civil society or professional ICT-oriented organizations, shall
20 be jointly responsible for the creation of general implementing rules and regulations (IRR) of
21 this Act. The Solicitor-General shall participate to ensure that the IRR is not in conflict with
22 this Act, with other laws, with other IRRs of this Act, and with generally accepted principles
23 of international human, civil, and political rights.

24 (b) The General Implementing Rules and Regulations for the Implementation of the
25 Magna Carta for Philippine Internet Freedom shall be made public after its approval.

26 (c) The President shall implement the General Implementing Rules and Regulations
27 for the Implementation of the Magna Carta for Philippine Internet Freedom through the
28 applicable agencies and instrumentalities of the Executive.

29 *Section 51. Implementing Rules and Regulations for Information and Communications*
30 *Technology Infrastructure Development. –*

1 (a) The Secretary of Information and Communication Technology, the Secretary of
2 Finance, the Director-General of the National Economic and Development Authority, and
3 the Chairman of the Board of Investments, or their duly authorized and appointed
4 delegates, an appointee from civil society or professional ICT-oriented organizations, and an
5 appointee from the business sector shall be jointly responsible for the creation of
6 implementing rules and regulations (IRR) of this Act towards the development of
7 information and communications technology infrastructure. The Solicitor-General shall
8 participate to ensure that the IRR is not in conflict with this Act, with other laws, with other
9 IRRs of this Act, and with generally accepted principles of international human, civil, and
10 political rights.

11 (b) The IRR for ICT Infrastructure Development shall be made public after its
12 approval.

13 (c) The President shall implement the IRR for Information and Communications
14 Technology Infrastructure Development through the applicable agencies and
15 instrumentalities of the Executive.

16 *Section 52. Implementing Rules and Regulations for Cybercrime Law Enforcement. –*

17 (a) The Secretary of Information and Communication Technology, the Secretary of
18 Justice, the Secretary of Interior and Local Government, the Secretary of Social Welfare and
19 Development, the Secretary of Foreign Affairs, the Director-General of the National Bureau
20 of Investigation, and the Director-General of the Philippine National Police, or their duly
21 authorized and appointed delegates, an appointee from the academe, an appointee from
22 civil society, and an appointee from a professional ICT-oriented organization shall be jointly
23 responsible for the creation of implementing rules and regulations (IRR) of this Act towards
24 cybercrime and law enforcement. The Solicitor-General and the Chairman of the
25 Commission on Human Rights shall participate to ensure that the IRR is not in conflict with
26 this Act, with other laws, with other IRRs of this Act, and with generally accepted principles
27 of international human, civil, and political rights.

28 (b) The IRR for Cybercrime and Law Enforcement shall be made public after its
29 approval.

30 (c) The President shall implement the IRR for Cybercrime and Law Enforcement
31 through the applicable agencies and instrumentalities of the Executive.

32 *Section 53. Implementing Rules and Regulations for Information and Communications*
33 *Technology Education, Training, and Human Resources. –*

1 (a) The Secretary of Information and Communication Technology, the Secretary of
2 Education, the Secretary of Science and Technology, the Commissioner of Higher Education,
3 the Director-General of the Technical Education and Skills Development Authority, the Head
4 of the National Telecommunications Training Institute, or their duly authorized and
5 appointed delegates, and an appointee from the academe shall be jointly responsible for
6 the creation of implementing rules and regulations (IRR) of this Act towards information and
7 communications technology education, training and human resources. The Solicitor-General
8 and the Secretary of Labor and Employment shall participate to ensure that the IRR is not in
9 conflict with this Act, with other laws, with other IRRs of this Act, and with generally
10 accepted principles of international human, civil, and political rights.

11 (b) The IRR for ICT Education, Training and Human Resources shall be made public
12 after its approval.

13 (c) The President shall implement the IRR for ICT Education, Training and Human
14 Resources through the applicable agencies and instrumentalities of the Executive.

15 *Section 54. Implementing Rules and Regulations for Information and Communications*
16 *Technology Research and Development. –*

17 (a) The Secretary of Information and Communication Technology, the Secretary of
18 Science and Technology, the Director-General of the National Economic and Development
19 Authority, or their duly authorized and appointed delegates, an appointee from the
20 academe, and an appointee from the business sector, shall be jointly responsible for the
21 creation of implementing rules and regulations (IRR) of this Act towards information and
22 communications technology research and development. The Solicitor-General shall
23 participate to ensure that the IRR is not in conflict with this Act, with other laws, with other
24 IRRs of this Act, and with generally accepted principles of international human, civil, and
25 political rights.

26 (b) The IRR for ICT Research and Development shall be made public after its
27 approval.

28 (c) The President shall implement the IRR for ICT Research and Development through
29 the applicable agencies and instrumentalities of the Executive.

30 *Section 55. Implementing Rules and Regulations for National Cyberdefense,*
31 *Cyberintelligence, Counter-Cyberterrorism, and Counter-Cyberespionage. –*

32 (a) The Secretary of National Defense, the Secretary of Interior and Local
33 Government, or their duly authorized and appointed delegates, the Chief of Staff of the

1 Armed Forces of the Philippines (AFP), the commanding general of the unit of the Philippine
2 Air Force tasked with national cyberdefense, the commanding officer of the Intelligence
3 Service, Armed Forces of the Philippines (ISAFP), the commanding officer of the
4 Communication Electronics and Information Systems Service, Armed Forces of the
5 Philippines (CEISSAFP), and the Director-General of the Philippine National Police shall be
6 jointly responsible for the creation of implementing rules and regulations (IRR) of this Act
7 towards ensuring national cyberdefense, cyberintelligence, counter-cyberterrorism, and
8 counter-cyberespionage. The Secretary of Information and Communication Technology shall
9 provide technical advice. The Solicitor-General and the Chairman of the Commission on
10 Human Rights shall participate to ensure that the IRR is not in conflict with this Act, with
11 other laws, with other IRRs of this Act, and with generally accepted principles of
12 international human, civil, and political rights.

13 (b) The IRR for National Cyberdefense, Cyberintelligence, Counter-Cyberterrorism,
14 and Counter-Cyberespionage shall be made public after its approval.

15 (c) Subject to the approval of the President, and subject to the advice and consent of
16 the Joint Select Committee on Military and Intelligence Affairs of the House of
17 Representatives and the Senate, the Secretary of National Defense, the Secretary of Interior
18 and Local Government, or their duly authorized and appointed delegates, the Chief of Staff
19 of the Armed Forces of the Philippines (AFP), the commanding general of the unit of the
20 Philippine Air Force tasked with national cyberdefense, the commanding officer of the
21 Intelligence Service, Armed Forces of the Philippines (ISAFP), the commanding officer of the
22 Communication Electronics and Information Systems Service, Armed Forces of the
23 Philippines (CEISSAFP), and the Director-General of the Philippine National Police shall
24 prepare a National Cyberdefense and Cybersecurity Plan every three years.

25 (d) The President shall have the power to implement the National Cyberdefense and
26 Cybersecurity Plan.

27 (e) The contents of the current and past National Cyberdefense and Cybersecurity
28 Plans shall be covered by executive privilege and shall be considered state secrets, and any
29 unauthorized disclosure shall be punishable to the fullest extent possible by relevant laws.

30
31 *Section 56. Implementing Rules and Regulations for the Provision of Free Wifi Access. –*

32 The Secretary of Information and Communication Technology, Secretary of Tourism
33 and the Secretary of Finance shall formulate and promulgate the implementing rules and
34 regulations of this Act towards the designation of selected public areas for free wifi access.

35 *Section 57. Periodic Review of the Implementing Rules and Regulations of the Magna Carta*
36 *for Philippine Internet Freedom. –*

1 (a) Mandatory and periodic reviews of the implementing rules and regulations of the
2 Magna Carta for Philippine Internet Freedom shall be done by the offices designated by this
3 Act to create implementing rules and regulations. Such reviews shall be performed no less
4 than every three years and no more than every five years, to keep pace with technological
5 advancements and other changes.

6 (b) Periodic reviews of the implementing rules and regulations and the
7 recommendation of the improvement of the Magna Carta for Philippine Internet Freedom
8 shall be done by the offices designated by this Act to create implementing rules and
9 regulations, to keep pace with technological advancements and other changes.

10 **Part 9. Final Provisions.**

11 *Section 58. Appointment of the Secretary of Information and Communications Technology. –*
12 Subject to confirmation by the Commission on Appointments, the President shall appoint
13 the Secretary of Information and Communications Technology within 30 days of the
14 effectivity of this Act.

15 *Section 59. Release of Initial Appropriations. –* Subject to government budgetary and audit
16 procedures, the Department of Budget and Management shall release appropriations to the
17 Secretary of Information and Communications Technology for purposes of implementing
18 this Act within 30 days of his appointment.

19 *Section 60. Preparation of Implementing Rules and Regulations. –* Within 90 days of the
20 release of initial appropriations, implementing rules and regulations shall have been
21 prepared and approved. The National Cyberdefense and Cybersecurity Plan shall be
22 prepared, approved, and implemented within 90 days of the approval of the implementing
23 rules and regulations.

24 *Section 61. Compliance of Government ICT Infrastructure and Critical Networks, Data, and*
25 *Internet Infrastructure. –*

26 (a) Within 180 days of the approval of the implementing rules and regulations,
27 government agencies and instrumentalities shall have secured their private network and
28 data infrastructure. Penalties as prescribed by this Act shall be imposed for noncompliance.

29 (b) Within 270 days of the approval of the implementing rules and regulations,
30 government agencies and instrumentalities shall have secured their public network, data,
31 and Internet infrastructure. Penalties as prescribed by this Act shall be imposed for
32 noncompliance.

1 (c) Within one (1) year of the approval of the implementing rules and regulations, all
2 Internet service providers, Internet exchanges, Internet data centers, Internet gateway
3 facilities, telecommunications entities, and persons providing Internet connection, network,
4 or data transmission services shall have met the minimum standards of privacy and security
5 for their private and public network, data, and Internet infrastructure. Penalties as
6 prescribed by this Act shall be imposed for noncompliance.

7 (d) Within 90 days of the approval of the implementing rules and regulations, all
8 Internet service providers, Internet exchanges, Internet data centers, Internet gateway
9 facilities, telecommunications entities, and persons providing Internet connection, network,
10 or data transmission services shall have met the minimum standards of interconnectivity
11 and interoperability of their information and communications technology infrastructure.
12 Administrative penalties shall be prescribed for noncompliance.

13 (e) Within 180 days of the approval of the implementing rules and regulations, all
14 Internet service providers, Internet exchanges, Internet data centers, Internet gateway
15 facilities, telecommunications entities, and persons providing Internet connection, network,
16 or data transmission services shall have met the minimum standards of service quality.
17 Administrative penalties shall be prescribed for noncompliance.

18 *Section 62. Public Information Campaign for the Magna Carta for Philippine Internet*
19 *Freedom and its Implementing Rules and Regulations. –*

20 (a) The Office of the President, the Presidential Communications Development and
21 Strategic Planning Office or its successor agency, the Philippine Information Agency or its
22 successor agency, and the Department of Interior and Local Government through the
23 information offices of local government units, shall be jointly responsible for information
24 campaigns to ensure nationwide awareness of the Magna Carta for Philippine Internet
25 Freedom and its implementing rules and regulations.

26 (b) The Department of Education and the Department of Social Welfare and
27 Development may provide age-appropriate information campaigns in schools to ensure
28 nationwide awareness of the Magna Carta for Philippine Internet Freedom, its
29 implementing rules and regulations, and the safe use of the Internet and information and
30 communications technology for children of school age and for out-of-school youths.

31 *Section 63. Initial Funding Requirements. –*

32 (a) DICT – An initial appropriation of fifteen million pesos (PHP 15,000,000) shall be
33 drawn from the national government for purposes of establishment and operation of the

1 DICT, exclusive of the existing appropriations of its subordinate agencies, which shall accrue
2 to the DICT budget.

3 (b) DOJ – The initial funding requirements for the implementation of this Act of the
4 DOJ shall be charged against the current appropriations of the DOJ.

5 (c) NBI – The initial funding requirements for the implementation of this Act of the
6 NBI shall be charged against the current appropriations of the NBI.

7 (d) PNP – The initial funding requirements for the implementation of this Act of the
8 PNP shall be charged against the current appropriations of the PNP.

9 (e) IRR – An initial appropriation of five million pesos (PHP 5,000,000), to be
10 disbursed by the Secretary of Information and Communications Technology, shall be drawn
11 from the national government for purposes of the preparation of the Implementing Rules
12 and Regulations of this Act.

13 (f) PIA – An appropriation of five million pesos (PHP 5,000,000) may be drawn from
14 the national government for purposes of the information dissemination campaign on this
15 Act by the PIA.

16 (g) Other agencies – The initial funding requirements for the implementation of this
17 Act by other agencies shall be charged against the current appropriations of the respective
18 agencies.

19 *Section 64. Succeeding Appropriations.* – Such sums as may be necessary for the
20 implementation of this Act shall be included in the agencies' yearly budgets under the
21 General Appropriations Act.

22 *Section 65. Separability Clause.* – If any provision or part hereof is held invalid or
23 unconstitutional, the remainder of the law or the provisions not otherwise affected shall
24 remain valid and subsisting.

25 *Section 66. Repealing Clause.* – Any law, presidential decree or issuance, executive order,
26 letter of instruction, administrative order, rule, or regulation contrary to, or inconsistent
27 with, the provisions of this Act is hereby repealed, modified, or amended accordingly.

28 *Section 67. Effectivity Clause.* – This Act shall take effect fifteen (15) days after its online
29 publication in the Official Gazette. Within seven (7) days after its online publication, this Act
30 shall be published on (2) newspapers of general circulation.

31 *Approved,*