Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

SEVENTEENTH (17TH) CONGRESS
First Regular Session

House Bill No. 1378

Introduced by: Rep. BERNADETTE R. HERRERA-DY

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

EXPLANATORY NOTE

It is the policy of the State to give priority to science and technology to foster patriotism and nationalism, accelerate social progress, and promote total human liberation and development;[1] broaden scientific and technological knowledge;[2] and recognize that science and technology are essential for national development and progress.[3] The State shall give priority to research and development, invention, innovation, and their utilization; and to science and technology education, training, and services.[4] The State shall encourage the widest participation of private groups, local governments, and community-based organizations in the generation and utilization of science and technology.[5]

The Internet and social media have become integral to ensuring transparency, accountability, and good governance in the Philippines and in 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. 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.

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 (BPO) and Knowledge Process Outsourcing (KPO) industries,

[1] *See* Phil. Const. art. 2 § 17.
[2] *See id.* art. XIV § 3(1).
[3] *See id.* art. XIV § 10.
[4] *See id.*
[5] *See id.* art. XIV § 12.

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.

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.

This bill borrows from and builds upon S.B. 3327 (15th Congress) authored by Sen. Miriam Defensor-Santiago and S.B. 1091 (16th Congress) authored by Sen. Bam Aquino. Among the particular items of the bill, we wish to push for a provision that makes free WIFI (also: wireless local areas network or WLAN) 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. For instance, as defined in Part I Section 2 (f): "The Internet has the potential to become a theater of war, and that ICT can be developed into weapons of mass destruction; thus, consistent with the national interest and the Constitution, the State shall pursue a policy of no first use of cyber weapons against foreign nations, and shall implement plans, policies, programs, measures, and mechanisms to provide cyber defense of Philippine Internet and ICT infrastructure resources." The MCPIF also tackles such issues as hacking, Internet libel, hate speech, child pornography, cyber crime, human trafficking, and a host of other issues. In recognition of the newly created Department of Information and Communications Technology (DICT) under R.A. 10844, this version deletes references to DICT which were present in prior versions of similar MCPIF bills filed in the previous Congress.

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

BERNADETTE HERRERA-DY

Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City

SEVENTEENTH (17TH) CONGRESS
First Regular Session

House Bill No. 1378

Introduced by: Rep. BERNADETTE R. HERRERA-DY

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

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

Part I. General Provisions.

Section 1. Short Title. - This Act shall be known as "The Magna Carta for Philippine Internet Freedom of 201_."

Section 2. Declaration of Policy. -

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

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

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

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

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

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

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

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

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

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

(k) Art and culture can be created on devices, on networks, and on the Internet; thus, the State shall pursue a policy that promotes the Internet and information and

communications technology, and the innovation therein and thereof, as instruments of life, liberty, and the pursuit of happiness.

Part 2. Definition of Terms

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

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

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

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

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

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

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

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

(f) Botnet - A network of computers infected with bots.

(g) Cache - A temporary storage of recently accessed data or information, which may be stored in the local storage medium of a device or computer, or in the storage media of a network, for purposes of speeding up subsequent retrievals of data or information from the Internet or networks.

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

(i) Code - The symbolic arrangement of data or instructions in a computer program or a set of such instructions.

(j) Component - Any individual part of a device.

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

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

(m) Configuration - The way a device, computer, computer system, or network is set up.

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

(o) Control - The use of resources, modification of the configuration, and otherwise exertion of a directing influence on the operation of a device, computer, system, or network.

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

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

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

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

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

(u) Cybercrime - Any unlawful act punishable by this law or other relevant laws committed through or using the Internet or information and communications technology.

(v) Cyber defense - The collection of plans, policies, programs, measures, mechanisms, and weapons designed to defend the Philippines from cyber attack.

(w) Cyber intelligence - The collection, analysis, processing, and dissemination of information, which may be done through or using the Internet or information and communications technology, designed to provide guidance and direction to commanders and leaders of military and law enforcement units towards the combating of acts of cyber attack and cyber terrorism.

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

(y) Cyberspace - A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers, or the virtual space constituted by a computer network with a set of distributed applications and its users.

(z) Cyberterrorism - A violation of the Human Security Act of 2007 committed through or using the Internet or information and communications technology.

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

(ab) Data - The reinterpretable representation of information in a formalized manner suitable for communication, Interpretation, or processing, or information represented in a manner suitable for automatic processing.

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

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

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

(ac) Device - The material element or assembly of such elements intended to perform a required function.

(ad) Download - The transfer of data or information from the Internet or a network to a device or computer upon request of the user for this information.

(ae) Encryption - An encoding scheme that produces meaningless information to all observers except those with the decryption key made for the purpose.

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

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

(i) Data processing equipment - Equipment used to process data electronically.

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

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

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

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

(aj) Hardened - The state of reduced vulnerability to unauthorized access or control or to malicious attacks of a device, computer, network, or information and communications technology infrastructure.

(ak) Hardware - The collection of physical elements that comprise a device, equipment, computer, system, or network.

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

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

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

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

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

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

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

(ii) Sensitive private information - Refers to personal information:

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

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

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

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

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

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

(ap) Internet - The global system of interconnected computer networks linked by various telecommunications technologies and that uses the standard internet protocol suite.

(aq) Medium - A material used for specific purposes.

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

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

(ar) Network - A collection of computers, devices, equipment, and other hardware interconnected by communication channels that allow sharing of resources and information.

(i) Open network - A network, such as the Internet, which allows any entity or device to interconnect with freely at" any time and become a user or part of the network, provided the entity or device uses the same or compatible communications protocols, and which allows any user to cease

interconnectivity with freely at any time, provided the user does so in a manner that does not compromise the security protocols of the open network or of other users.

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

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

(as) Offline - The state of being disconnected from the Internet or networks.

(at) Online - The state of being connected to the Internet or a network.

(au) Ownership - Ownership is defined by the Civil Code.

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

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

(av) Physical plant - The building, structure, and infrastructure necessary to support and maintain a facility.

(aw) Platform - The hardware architecture and/ or software framework, including application frameworks, whose combination allows a user to run software.

(ax) Privacy - May refer to any of these definitions, or a combination of these definitions:

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

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

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

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

(ay) Privilege - A right that, When granted to an entity, permits the entity to perform an action.

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

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

(az) Processing - The act of performing functions or activities on data or information.

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

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

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

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

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

(bc) Script - A computer program or sequence of instructions that is interpreted or carried out by another computer program instead of directly by a computer, device, or equipment.

(bd) Security - The ability to prevent fraud as well as the protection of information availability, integrity and confidentiality.

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

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

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

(be) Service - A set of functions offered to a user by another person or by an organization.

(bf) Service quality - The collective effect of service performance which determines the degree of satisfaction of a user of the service.

(bg) Software - The set of programs, procedures, algorithms and its documentation concerned with the operation of a data processing system, computer, device, or equipment.

(bh) Software application - Software designed to help a user perform a specific task or set of tasks.

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

(bj) Telecommunications - A service or system of interconnected entities providing the ability to exchange and interchange data between points or from a point to multiple points.

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

(bl) Upload - The transfer of data or information to the Internet or a network from a device or computer, initiated by the user.

(bm) Uptime - The time a device, equipment, computer, or network can be left unattended without suffering failure, or needing to be undergo administrative or maintenance purposes.

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

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

Part 3. Internet Rights and Freedoms

Section 4. Right to freedom of speech and expression on the Internet. -

(a) The State shall, within its jurisdiction:

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

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

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

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

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

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

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

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

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

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

Section 5. Promotion of universal access to the Internet.

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

(b) A person's right to unrestricted access to the Internet may, upon discretion of the appropriate Cybercrime Court whose jurisdiction is defined in this Act, be suspended as an accessory penalty. Upon final convictiOl1 for any of the following criminal offenses:

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

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

(iii) Any criminal offense defined and punishable by this Act. The right of person accused of any of the above offenses to unrestricted access to the Internet may be suspended or limited by the court of competent jurisdiction pending final judgment upon a showing, following notice and hearing, that there is a strong likelihood that the accused will be able to facilitate the commission of the offense so charged unless such order were issued.

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

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

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

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

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

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

(f) The State, through the Department of Information and Communication Technology in coordination with the Department of Tourism, Commission on Higher Education, and Local Government Units, shall provide free WIFI access in designated public areas. This provision does not prejudice the Department of Information and Communication Technology from partnering with private entities to accomplish this goal.

(g) These public areas may include but not be limited to the following:

1. common areas of local government offices;
2. train stations;
3. bus stations;
4. tourism spots;
5. National Heritage spots;
6. public parks; and
7. designated areas within State Universities and Colleges.

Section 6. Right to privileged access to and control of devices. -

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

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

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

Section 7. Protection of the freedom to innovate and create without permission. -

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

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

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

Section 8. Right to privacy of data. -

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

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

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

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

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

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

Section 9. Right to security of data. -

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

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

(c) No third party shall be granted access to the private data or networks of a person by an Internet service provider, telecommunications entity, or such person providing Internet or data services, except upon a final court order issued in accordance with Section 5 of this Act. It shall be a condition precedent to the filing of such action for access to private data that the person owning such data be first properly notified of such a request by the Internet service

provider, telecommunications entity, or such person providing Internet or data services, and that such person has refused to grant the requested access. A person shall not be deemed to have been properly notified unless the person has acknowledged the notification of the request for access and has agreed to grant or refuse access.

(d) No third party granted the right to access the private data or networks of a person by an Internet service provider, telecommunications entity, or other such person providing Internet or data services, shall be given any property rights over the data being accessed, the media where the private data is stored, the equipment through which the network is run or maintained, or the physical plant where the network equipment is housed, beyond the right to access the private data or network, unless otherwise granted such rights by the courts following the appropriate action and final order.

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

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

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

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

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

Section 10. Protection of intellectual property. -

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

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

(c) Subject to the Intellectual Property Code of the Philippines (RA 8293), as amended, and other relevant laws, no Internet service provider, telecommunications entity, or such person providing Internet or data services shall have intellectual property rights over derivative content that is the result of creation, invention, innovation, or modification by a person using the service provided by the Internet service provider, telecommunications entity, or such person providing Internet or data services, unless such content is a derivative work of content already owned by or assigned to the Internet service provider, telecommunications entity, or such person providing Internet or data services acting as a content provider. The exception to the intellectual property rights of the person must be explicitly provided for via an end user license agreement to which both parties have agreed, and the existence of the derivative content must be dependent on the service provided by the Internet service provider, telecommunications entity, or such person providing Internet or data services.

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

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

Section 11. Protection of the Internet as an open network. -

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

(b) No person or entity shall restrict or deny the interconnection or inter operability of a device, an equipment, or a network that is capable of such interconnection or inter operability to the Internet, to other public networks, or to .other Internet service providers, telecommunications entities, or other such persons providing Internet or data services, without due process of law or authority vested by law. Provided, Customer premises equipment as redefined by this Act, shall not be covered by the requirements under this

Section. Provided, further, The inter operability of a device, an equipment, or a network within a private network may be restricted by the duly authorized system and/or network administrators of the private network, subject to the provisions of the Data Privacy Act of 2012 (RA 10173) and other relevant laws.

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

(a) if the data or information whose flow is being favored is used to solely to manage the security or service quality of a network, or of an Internet or data service, and;

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

Section 13. Promotion of the use of the Internet and information and communications technology for purposes of transparency in governance and freedom of information. -

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

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

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

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

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

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

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

(c) The State shall ensure that any format used for the files available for download are in common use, platform independent, machine readable, or is based on an underlying open standard, developed by an open community, affirmed and maintained by a standards body and such open standard must be fully documented and publicly available. Such files must be:

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

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

(iii) Have their authenticity verifiable through a check sum standard determined by the Internet Engineering Task Force or similar globally reputable organization. The Bureau of Product Standards of the Department of Trade and Industry shall be responsible for setting the standards for the file formats to be used by the State in the publication of government public information, in accordance with the provisions of this Act.

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

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

Section 14. Declaration of Compliance with Treaty Obligations and International Conventions. -

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

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

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

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

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

Section 15. The State as the Primary Duty Bearer. - The State, as the primary duty-bearer, shall uphold constitutional rights, privileges, guarantees, and obligations in the development and implementation of policies related to the Internet and information and

communication technology. The State shall fulfill this duty through law, policy, regulatory instruments, administrative guidelines, and other appropriate measures, including temporary special measures.

Section 16. Duties of the State Agencies and Instrumentalities. -

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

(b) Cybercrime Law Enforcement. - Subject to provisions of this Act, the Department of Justice, The Department of Interior and Local Government, the Department of Social Welfare and Development, the Department of Information and Communications Technology, the National Bureau of Investigation, and the Philippine National Police shall be jointly responsible over the development and implementation of plans, policies, programs, measures, and mechanisms for cybercrime law enforcement in the Philippines.

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

(d) Information and Communications Technology Infrastructure Development. -

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

(ii) ICT infrastructure and facilities, including the civil works components thereof, fall within private sector infrastructure or development projects as defined under Republic Act No. 6957, as amended by Republic Act No. 7718, and may, upon the discretion of the National Government or local government units, be the subject of the contractual arrangements authorized under the said law. Provided, that the DICT shall be the implementing agency of such projects to be implemented by the national government; Provided, further, that the DICT shall have the right to require its prior

concurrence to such projects implemented by local government units, through duly promulgated regulations that specify, among others, the requisite threshold contract prices that would require prior concurrence of the DICT.

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

(iv) The development and operation of information and communications technology infrastructure and facilities is hereby declared as a preferred area of investment and shall be included in the annual Investment Priority Plan issued in accordance with the Omnibus Investments Code. Subject to the contrary factual determination of the Board of Investments, an entity involved in the development and operation of information and communications technology infrastructure and facilities is presumed to be entitled to register as a registered enterprise under the Investment Priorities Plan; Provided, that an enterprise that proposes to operate a public utility or public service shall be subject to the equity requirements imposed by the Constitution and by applicable laws; Provided, further, that any such entity which intends to operate in a special economic zone or in a tourism economic zone as defined by applicable law shall be entitled to receive the additional investment incentives granted to such zone- registered enterprises in accordance with the applicable law; Provided, finally, that nothing in this Section shall be construed to limit the available incentives to which an entity may be entitled to under Republic Act No. 6957, as amended.

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

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

(e) Human Resources, Skills and Technology Development for Information and Communications Technology. - Subject to provisions of this Act, the Department of Information and Communications Technology, the Department of Science and Technology,

and the Technical Education and Skills Development Authority shall have the joint responsibility to develop and implement plans, policies, programs, measures, and mechanisms for the development of human resources, skills development, and technology development for information and communications technology infrastructure in the Philippines.

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

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

Section 17. Amendments to the Public Telecommunications Policy Act o/the Philippines.-

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

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

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

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

b) Ensure quality, safety, reliability, security, compatibility and interoperability of telecommunications, NETWORK, AND INTERNET services in conformity with standards and specifications set by international radio, telecommunications, NETWORK, AND INTERNET organizations to which the Philippines is a signatory;

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

xxx

e) Promote consumers' welfare by facilitating access to telecommunications, NETWORK, AND INTERNET SERVICES whose infrastructure and network must be geared towards the needs of individual and business users, AND BY DEVELOPING AND IMPLEMENTING STANDARDS, PLANS, POLICIES, PROGRAMS, MEASURES, AND MECHANISMS, INCLUDING ARBITRATION, QUASI-JUDICIAL, AND PROSECUTORIAL MECHANISMS, TO PROTECT THE WELFARE OF CONSUMERS AND USERS OF TELECOMMUNICATIONS, NETWORK, AND INTERNET SERVICES;

xxx

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

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

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

xxx

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

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

xxx

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

SECTION 10A. LOCAL INTERNET SERVICE PROVIDER. - A LOCAL INTERNET SERVICE PROVIDER SHALL:

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

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

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

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

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

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

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

SECTION 10B. INTERNET EXCHANGE. - THE NUMBER OF ENTITIES ALLOWED TO PROVIDE INTERNET EXCHANGE SERVICES SHALL NOT BE LIMITED, AND AS A MATTER OF POLICY, WHERE IT IS ECONOMICALLY VIABLE, AT LEAST TWO (2) INTERNET EXCHANGES SHALL BE AUTHORIZED: PROVIDED, HOWEVER, THAT A LOCAL INTERNET

SERVICE PROVIDER SHALL NOT BE RESTRICTED FROM OPERATING ITS OWN INTERNET EXCHANGE SERVICE IF ITS VIABILITY IS DEPENDENT THERETO. SUCH INTERNET EXCHANGE SHALL HAVE THE FOLLOWING OBLIGATIONS:

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

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

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

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

(A) IT SHALL INTERCONNECT WITH ALL OTHER INTERNET DATA CENTERS IN THE SAME CATEGORY AND WITH ALL LOCAL INTERNET SERVICE PROVIDERS AND OTHER TELECOMMUNICATIONS ENTITIES, UPON APPLICATION AND

WITHIN A REASONABLE TIME PERIOD, AND UNDER FAIR AND REASONABLE LEVEL CHARGES, IN ORDER THAT INTERNET AND NETWORK SERVICES ARE MADE POSSIBLE; AND

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

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

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

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

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

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

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

SUBJECT TO THE NATURE OF THE CONTENT THAT IS PROVIDED BY THE CONTENT PROVIDER FOR COMMERCIAL PURPOSES, LAWS SUCH AS PAGCOR CHARTER, AS AMENDED, THE MTRCB CHARTER, AS AMENDED, AND OTHER RELEVANT LAWS, SHALL BE DEEMED APPLICABLE TO THE CONTENT PROVIDER.

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

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

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

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

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

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

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

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

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

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

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

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

XXX

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

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

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

(f) Thorough and prompt investigation of, and action upon complaints. The utility shall endeavor to allow complaints [over the telephone] TO BE RECEIVED BY POST AND OVER MEANS USING TELECOMMUNICATIONS FACILITIES OR THE INTERNET, WHICH SHALL INCLUDE BUT SHALL NOT BE LIMITED TO VOICE CALLS, SHORT MESSAGE SERVICE (SMS) MESSAGES, MULTIMEDIA MESSAGE SERVICE (MMS) MESSAGES, OR EMAIL, and shall keep a record of all [written or phoned-in] complaints received and the actions taken to address these complaints;

SUBJECT TO THE FILING OF A FORMAL REQUEST TO THE UTILITY, A USER MAY REQUEST THE IMMEDIATE TERMINATION OF SERVICE, WITHOUT THE IMPOSITION OF FEES OR PENALTIES, AND WITH THE REFUND OF ANY FEES OR CHARGES ALREADY PAID BY THE USER, SHOULD A UTILITY NOT CONSISTENTLY COMPLY WITH PRECEDING

PARAGRAPHS (All (D), (E), (F), OR ANY OTHER MINIMUM PERFORMANCE STANDARDSSET BYTHE COMMISSION.

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

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

(2) THE UTILITY HAS EVIDENCE THAT THE NON-COMPLIANCE HAS NOT RECURRED. IS NOT RECURRING. NOR WILL RECUR IN THE FUTURE: OR THE UTILITY HAS EVIDENCE: THAT THE NON COMPLIANCE WAS DUE TO FACTORS BEYOND ITS CONTROL; OR THE UTILITY HAS PROVIDED IMMEDIATE REFUND OR REBATE TO THE USER UPON DEECTION OF THF NONCOMPLIANCE OR THE UTILITY HAS EVIDENCE THAT IT HAS EXERTED ITS BEST EFFORTS TO RESOLVE THE NONCOMPLIANCE AND RESTORE THE SERVICE TO THE LEVEL AGREED BETWEEN THE UTILITY AND THE USER WITHIN SEVEN (7) DAYS OF THE REQUEST FOR IMMEDIATE TERMINATION; AND THE UTILITY SHALL COMPLY WITH IMMEDIATE TERMINATION OF SERVICE, WITHOUT THE IMPOSITION OF FEES OR PENALTIES, AND REFUND ANY FEES OR CHARGES ALREADY PAID BY THE USER WITHOUT NEED FOR DEMAND SHOULD THE SERVICE NOT BE RESTORED WITHIN THE SEVEN (7) DAY PERIOD, WITHIN THREE (3) DAYS AFTER THE TERMINATION OF SERVICE.

SUBJECT TO STANDARDS SET BY THE COMMISSION, PENALTIES MAY BE IMPOSED ON A UTILITY THAT IS UNABLE TO COMPLY WITH PRECEDING PARAGRAPHS (B) AND (C). THE COMMISSION MAY IMPOSE

ADDITIONAL PENALTIES IF THE UTILITY DOES NOT REFUND ANY DEPOSITS, FEES, OR CHARGES ALREADY PAID BY THE USER WITHOUT NEED FOR DEMAND WITHIN THREE (3) DAYS AFTER THE DEADLINE AGREED UPON BETWEEN THE USER AND THE UTILITY.

Section 18. Quality of Service and Network Fair Use. -

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

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

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

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

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

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

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

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

(b) Nothing in this section shall be construed as to prevent an Internet service provider, Internet exchange, Internet data center, Internet gateway facility, telecommunications entity, or person providing Internet connection, network, or data transmission services from taking reasonable and nondiscriminatory measures:

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

(ii) To give priority to emergency communications;

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

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

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

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

Section 19. Amendments to the Intellectual Property Code of the Philippines. -

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

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

xxx

(n) CODE, SCRIPTS, COMPUTER PROGRAMS, SOFTWARE APPLICATIONS, AND OTHER SIMILAR WORK, WHETHER

EXECUTABLE IN WHOLE OR AS PART OF ANOTHER CODE, SCRIPT, computer programs, SOFTWARE APPLICATION OR OTHER SIMILAR WORK;

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

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

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

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

xxx

180.3. The submission of a literary, photographic or artistic work to a newspaper, magazine or periodical for publication, shall constitute only a license to make a single publication unless a greater right is expressly granted. IN THE CASE OF POSTING TO A WEBSITE OR AN ONLINE VERSION OF A NEWSPAPER, MAGAZINE, OR PERIODICAL, ENABLING ACCESS TO THE WHOLE OR PORTION OF THE WORK VIA AUTOMATIC CONTENT SYNDICATION OR

SEARCH RESULTS SHALL NOT CONSTITUTE VIOLATION OF THE LICENSE UNLESS THE CONTRARY IS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT BETWEEN COPYRIGHT OWNER AND PUBLISHER/HOST/SERVICE PROVIDER. If two (2) or more persons jointly own a copyright or any part thereof, neither of the owners shall be entitled to grant licenses without the prior written consent of the other owner or owners.

xxx

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

Section 182. Filing of Assignment or License OF COPYRIGHT. - An assignment or exclusive license may be filed in duplicate with the National Library upon payment of the prescribed fee for registration in books and records kept for the purpose. Upon recording, a copy of the instrument shall be returned to the sender with a notation of the fact of record. Notice of the record shall be published in the IPO Gazette.

xxx

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

Section 187. Reproduction of Published Work. -187.1. Subject to the provisions of Section 177 [and subject to the provisions] in relation to the provision of Subsection

187.2, the private reproduction of a published work in a single copy, where the reproduction is made by a natural person exclusively for research and private study, shall be permitted, without the authorization of the owner of copyright in the work.

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

xxx

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

xxx

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

xxx

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

Section 192. Notice of {Copyright] APPLICABLE ECONOMIC RIGHTS. - Each copy of a work published or offered for sale may contain a notice bearing the name of the copyright owner, and the year of its first publication, and, in copies produced after the creator's death, the year of such death. IN CASE OF FAILURE OF THE AUTHOR OR COPYRIGHT OWNER TO INDICATE THE LICENSE APPLICABLE FOR THE WORK, IT SHALL BE PRESUMED THAT THE COPYRIGHT OWNER ADOPTED COPYRIGHT UNLESS INTENT TO THE CONTRARY IS PROVEN.

Section 20. Content Fair Use. -

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

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

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

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

Section 22. Amendments to the Data Privacy Act. -

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

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

(b) Subsequent mentions of "National Privacy Commission" are hereby amended to be consistent with the amendment above.

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

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

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

Part 5. Cybercrimes and Other Prohibited Acts.

Section 24. Network sabotage. -

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

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

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

Section 25. Failure to Provide Reasonable Security for Data and Networks. -

(a) Failure to provide security. - It shall be unlawful for any Internet service provider, telecommunications entity, or other such person providing Internet or data services to

intentionally or unintentionally fail to provide appropriate levels of security for data, networks, storage media where data is stored, equipment through which networks are run or maintained, or the physical plant where the data or network equipment "is housed.

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

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

Section 26. Violation of Data Privacy. -

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

(b) Unauthorized modification. - It shall be unlawful for any person to intentionally modify data, networks, storage media where data is stored, equipment through which networks are run or maintained, the physical plant where the data or network equipment is housed, without authority granted by the Internet service provider, telecommunications entity, or other such person providing Internet or data services having possession or ~control of the~ data or network, or to intentionally modify intellectual property published on the Internet or on other networks without the consent of the person having ownership,

possession, or control of the intellectual property, or without legal grounds, even if the modification is performed without malice.

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

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

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

Section 27. Violation of Data Security. -

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

(b) Cracking. - It shall be unlawful for any unauthorized person to intentionally modify or to crack data, networks, storage media where data is stored, equipment through which networks are run or maintained, the physical plant where the data or network equipment is housed, or for any unauthorized person to intentionally modify intellectual property published on the Internet or on other networks. The unauthorized modification or cracking of data, networks, storage media where data is stored, equipment through which networks are run or maintained, the physical plant where the data or network equipment is housed, or unauthorized modification of intellectual property published on the Internet or on other networks, shall be presumed to be malicious.

(c) Phishing. -

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

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

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

Section 28. Illegal and Arbitrary Seizure. -

(a) Illegal Seizure. - It shall be unlawful for any person to seize data, information, or contents of a device, storage medium, network equipment, or physical plant, or to seize any device, storage medium, network equipment, or physical plant connected to the Internet or to telecommunications networks of another person without his consent, or to gain possession or control of the intellectual property published on the Internet or on public networks of another

person without his consent, except upon a final ruling from the courts, issued following due notice and hearing.

(b) Aiding and Abetting Illegal Seizure. -It shall be unlawful for any person to aid or abet the seizure of data, information, or contents of a device, storage medium, network equipment, or physical plant, or to seize any device, storage medium, network equipment, or physical plant connected to the Internet or to telecommunications networks of another person without his consent, or to gain possession or control of the intellectual property published on the Internet or on public networks of another person without his consent, except upon a final ruling from the courts, issued following due notice and hearing, allowing the person to perform such seizure, possession, or control.

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

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

Section 29. Infringement of Intellectual Property Rights. -

(a) Copyright infringement. -

(i) Subject to the Intellectual Property Code of the Philippines and the laws governing fair use, it shall be unlawful for any person to publish or reproduce on the Internet, in part or in whole, any content that he does not have any economic rights over, or does not acknowledge and comply with the terms of copyright or license

governing the intellectual property rights enjoyed by the content being published or reproduced, or falsely claims having intellectual property rights over the content he does not own.

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

(iii) Non-attribution or plagiarism of free license or public domain content shall constitute infringement, but shall not be subject to damages.

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

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

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

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

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

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

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

Section 31. ICT-Enabled Prostitution and ICT-Enabled Trafficking in Persons. -

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

(b) ICT-Enabled Trafficking in Persons.-

(i) The performance of acts prohibited by Section 5 of R.A. No. 920B, or the "Anti-Trafficking in Persons Act of 2003," 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) The commission of acts prohibited by the Anti-Trafficking in Persons Act of 2003, as amended, through or using devices, equipment, or physical plants connected to the Internet or to telecommunications networks shall be penalized by the applicable provisions of the Anti-Trafficking in Persons Act of 2003, as amended.

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

> Section 5. Acts that Promote Trafficking in Persons. - The following acts which promote or facilitate trafficking in persons, shall be unlawful:
>
> x x x
>
> (c) To advertise, publish, print, broadcast or distribute, or cause the advertisement, publication, printing, broadcasting or

distribution by any means, including the use of information AND COMMUNICATIONS technology and the Internet, of any brochure, flyer, or any propaganda material that promotes trafficking in persons, 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 PROMOTING TRAFFICKING IN PERSONS;

xxx

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

xxx

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

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

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

(ii) The commission of acts prohibited by the "Special Protection of Children Against Abuse, Exploitation and Discrimination Act," as amended, through or using

devices, equipment, or physical plants connected to the Internet or to telecommunications networks shall be penalized by the applicable provisions of the "Special Protection of Children Against Abuse, Exploitation and Discrimination Act," as amended.

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

(a) Internet libel. -

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

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

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

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

(v) Exceptions to internet libel. - The following acts shall not constitute internet libel:

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

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

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

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

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

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

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

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

(b) Internet hate speech.-

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

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

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

(c) *Internet child pornography.* -

(i) The performance of acts prohibited by Sections 4 and 5 of R.A. No. 9775, or the "Anti-Child Pornography Act of 2009," 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) The commission of acts prohibited by the Anti-Child Pornography Act of 2009, as amended, through or using devices, equipment, or physical plants connected to the Internet or to telecommunications networks shall be penalized by the applicable provisions of the Anti-Child Pornography Act of 2009, as amended.

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

> (e) To knowingly, willfully and intentionally provide a venue for the commission of prohibited acts as, but not limited to, dens, private rooms, cubicles, cinemas, houses or in establishments purporting to be a legitimate business; OR TO KNOWINGLY, WILLFULLY AND INTENTIONALLY PROVIDE DEVICES, EQUIPMENT, OR PHYSICAL PLANTS CONNECTED TO THE INTERNET OR TO TELECOMMUNICATIONS NETWORKS FOR THE PRIMARY PURPOSE OF PUBLICATION, OFFERING, PRODUCTION, SELLING, DISTRIBUTION, BROADCASTING, EXPORT, OR IMPORTATION OF CHILD PORNOGRAPHY;
>
> (f) For film distributors, theaters, INTERNET SERVICE PROVIDERS, and telecommunication companies,. by themselves or in cooperation with other entities, to distribute any form of child pornography;
>
> xxx

(d) *Internet child abuse*. -

(i) The performance of acts prohibited by Section 9 of 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) The commission of acts prohibited by the Special Protection of Children Against Abuse, Exploitation and Discrimination Act, as amended, through or using devices, equipment, or physical plants connected to the Internet or to telecommunications networks shall be penalized by the applicable provisions of the

Special Protection of Children Against Abuse, Exploitation and Discrimination Act, as amended.

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

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

(e) *Expression inimical to the public interest.* -

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

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

Section 34. Sabotage of critical networks and infrastructure, acts of cyberterrorism, and cyberespionage.

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

(b) Cyberterrorism. -

(i) The performance of acts prohibited by Sections 3, 4, 5, and 6 of the Human Security Act of 2007 (RA9732) as amended, and Sections 4, 5, 6, and 7 of the Terrorism Financing Prevention and Suppression Act of 2012 (RA 10168), or the 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) The commission of acts prohibited by the Human Security Act of 2007, as amended, through or using devices, equipment, or physical plants connected to the Internet or to telecommunications networks shall be penalized by the applicable provisions of the Human Security Act of 2007, as amended.

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

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

xxx

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

7. SECTION 2S (NETWORK SABOTAGE), SECTION 27 (VIOLATION OF DATA PRIVACY), AND SECTION 28 (VIOLATION OF DATA SECURITY) OF THE MAGNA CARTA FOR PHILIPPINE INTERNET FREEDOM COMMITTED AGAINST CRITICAL DATA, NETWORK, INTERNET, OR TELECOMMUNICATIONS INFRASTRUCTURE, WHETHER PUBLICLY OR PRIVATELY OWNED,

x x x

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

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

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

Section 4. Financing of Terrorism. -

xxx

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

ANY PERSON WHO, BY MEANS OF A DEVICE, STORAGE MEDIUM, NETWORK EQUIPMENT, OR PHYSICAL PLANT CONNECTED TO THE INTERNET OR TO TELECOMMUNICATIONS NETWORKS, OR IN CONNIVANCE WITH A THIRD PARTY WITH ACCESS TO THE SAME, SHALL KNOWINGLY, WILLFULLY, AND INTENTIONALLY FACILITATE THE ORGANIZATION OR DIRECTION OF OTHERS TO COMMIT THE FINANCING OF TERRORISM UNDER THE PRECEDING PARAGRAPHS SHALL LIKEWISE BE GUILTY OF AN OFFENSE AND SHALL SUFFER THE SAME PENALTY AS HEREIN PRESCRIBED.

xxx

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

Art. 117. Espionage. - The penalty of prision correccional shall be inflicted upon any person who:

x x x

2. WITHOUT AUTHORITY THEREFOR, OR EXCEEDING THE AUTHORITY GRANTED BY THE STATE, AND BY MEANS OF A DEVICE, EQUIPMENT, OR PHYSICAL PLANT CONNECTED TO THE INTERNET, TO TELECOMMUNICATIONS NETWORKS, A NETWORK OF THE STATE, A PRIVATE NETWORK, OR ANY PROTECTED DEVICE, COMPUTER, SYSTEM, OR NETWORK, OR IN CONNIVANCE WITH A THIRD PARTY WITH ACCESS TO THE SAME, SHALL USE THE INTERNET, TELECOMMUNICATIONS NETWORKS, NETWORKS

OF THE STATE, OR PRIVATE NETWORKS TO OBTAIN ANY DATA OR INFORMATION OF A CONFIDENTIAL NATURE RELATIVE TO THE DEFENSE OF THE PHILIPPINES OR ANY DATA OR INFORMATION CLASSIFIED BY LAW AS STATE SECRETS; OR

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

XXX

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

Section 35. Cyberwarfare and National Defense. -

(a) It shall be unlawful for any person, or military or civilian agency, or instrumentality of the State to initiate a cyberattack against any foreign nation, except in the event of a declaration of a state of war with the foreign nation.

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

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

Section 36. National Cybersecurity and Protection of Government Information and Communications Technology Infrastructure.

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

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

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

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

Section 37. Amendments to the AFP Modernization Act. - Section 5 of the AFP Modernization Act (RA 7898) shall be amended to include:

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

xxx

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

(1) DETECT, IDENTIFY, INTERCEPT AND ENGAGE, IF NECESSARY, ANY ATTEMPTED OR ACTUAL PENETRATION OR CYBERATTACK OF PHILIPPINE GOVERNMENT INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE, AS WELL AS CRITICAL INFORMATION AND COMMUNICATIONS

TECHNOLOGY INFRASTRUCTURE WITHIN PHILIPPINE JURISDICTION;

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

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

(E) DEVELOPMENT OF CYBERINTELLIGENCE CAPABILITY. - THE INTELLIGENCE SERVICE OF THE ARMED FORCES OF THE PHILIPPINES (ISAFP) OR ITS SUCCESSOR SERVICE, SHALL DEVELOP ITS CYBERINTELLIGENCE CAPABILITY. THE CYBERINTELLIGENCE CAPABILITY SHALL ENABLE THE AFP TO:

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

(2) PROVIDE CYBERINTELLIGENCE SUPPORT TO PHILIPPINE ARMED FORCES AND POLICE FORCES, AND;

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

(F) DEVELOPMENT OF GOVERNMENT AND MILITARY INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE HARDENED AGAINST CYBERATTACK. - THE COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEM SERVICE, ARMED FORCES OF THE PHILIPPINES (CEISSAFP) OR ITS SUCCESSOR SERVICE, SHALL CONTINUALLY ENSURE THAT

GOVERNMENT AND MILITARY INFORMATION AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE ARE HARDENED AGAINST CYBERATTACK.

xxx

Section 38. Counter-Cyberterrorism. -

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

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

(c) Subject to the provisions of an existing treaty to which the Philippines is a signatory and to any contrary provision of any law of preferential application, and subject to the concurrence of the Secretary of Justice and the Secretary of Foreign Affairs, the Director of the National Bureau of Investigation may cooperate with or request the cooperation of foreign or international law enforcement agencies in the detection, identification, pursuit, apprehension, and the gathering of evidence leading to the conviction of persons who, although physically outside the territorial limits of the Philippines, have committed or are attempting to commit acts of cyberterrorism within Philippine jurisdiction.

Section 39. Counter-Cyberespionage. -

(a) The National Intelligence Coordinating Agency, supported by applicable military, law enforcement, and government services, offices, and agencies, shall be the lead agency

responsible for plans, policies, programs, measures, and mechanisms to detect, identify, and prevent cyberespionage attempts and incidents.

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

Part 7. Penalties.

Section 40. Applicability of the Revised Penal Code and other special laws. - Nomenclature notwithstanding, the provisions of Book I of the Revised Penal Code shall apply suppletorily to the provisions of this Act, whenever applicable.

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

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

(a) Violation of Section 24 (a) (Direct network sabotage) - Shall be punished with imprisonment of prision correccional or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

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

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

(d) Violation of Section 25 (b) (Negligent failure to provide security) - Shall be punished with imprisonment of prision correccional or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

(e) Violation of Section 26 (a) (Unauthorized access) - Shall be punished with imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

(f) Violation of Section 26 (b) (Unauthorized modification) - Shall be punished with imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

(g) Violation of Section 26 (c) (Unauthorized granting of privileges) - Shall be punished with imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,OOO.00) but not more than Two million pesos (Php2,000,000.00).

(h) Violation of Section 26 (d) (Unauthorized disclosure) - imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

(i) Violations of the Section 26 (e) (Violation of Data Privacy Act through ICT)-

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

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

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

(iv) Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive Personal Information Due to Negligence through "ICT"- imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

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

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

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

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

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

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

(j) Violation of Section 27 (a) (Hacking) - imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

(k) Violation of Section 27 (b) (Cracking) - imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

(I) Violation of Section 27 (c) (phishing) - imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

(m) Violation of Section 27 (d) (Violation of Data Privacy Act with hacking, cracking, or phishing) -

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

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

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

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

(v) Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of Personal Information) with hacking, cracking, or phishing - shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Phpl00,000.00) but not more than Five hundred thousand pesos (Php500,000.00).

(vi) Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of Sensitive Personal Information) with hacking, cracking, or phishing - shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Phpl00,000.00) but not more than One million pesos(Php1,000,000.00).

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

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

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

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

(n) Violation of Section 28 (a) (Illegal seizure of ICT) - shall be punished with imprisonment of prision correccional or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

(o) Violation of Section 28 (b) (Aiding and abetting illegal seizure of ICT) - shall be 18 punished with imprisonment of prision correccional in its minimum period or a fine of not more than Four hundred thousand pesos (PhP400,000.00) or both.

(p) Violation of Section 28 (c) (Arbitrary seizure of ICT) - Shall be punished with imprisonment of prision correccional in its maximum period or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

(q) Violation of Section 28 (d) (instigating arbitrary seizure of ICT) - shall be punished with imprisonment of prision correccional or a fine of not more than Five hundred thousand pesos (PhP500,OOO.00) or both.

(r) Violation of Section 29 (a) (i) (Copyright infringement) - any person infringing a copyright shall be liable to pay to the copyright proprietor or his assigns or heirs such actual damages, including legal costs and other expenses, as he may have incurred due to the infringement as well as the profits the infringer may have made due to such infringement, and in proving profits the plaintiff shall be required to prove sales only and the defendant shall be required to prove every element of cost which he claims, or, in lieu of actual damages and profits, such damages which to the court shall appear to be just and shall not be regarded as penalty.

(s) Violation of Section 29 (a) (ii) (Plagiarism of copyleft) - The same penalty for a violation of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this Section.

(t) Violation of Section 29 (a) (iii) (Plagiarism of public domain content) - While this constitutes infringement, it shall not be subject to the payment of damages or to any other penalty.

(u) Violation of Section 29 (a) (iv) (Reverse engineering) - The same penalty for a violation of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this Section.

(v) Violation of Section 29 (b) (Piracy through ICT) - The same penalty for a violation of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this Section.

(w) Violation of Section 29 (c) (Cybersquatting) - The same penalty for a violation of Section 47 (a) (i) (Copyright infringement) shall be imposed for a violation of this Section.

(x) Violation of Section 29 (d) (Unreasonable restriction of device privileges) - shall be punished with a fine of not less than one hundred thousand pesos (Php 100,000.00) or more than two million pesos (PhP 2,000,000.00).

(y) Violation of Section 30 (Fraud via ICT) - shall be punished with imprisonment of prision correccional or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a maximum amount that is double the amount of damage incurred, whichever is higher, or both imprisonment and fine.

(z) Violation of Section 31 (a) (ICT-enabled prostitution) - shall be punished with imprisonment of prision mayor or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a maximum amount of Five hundred thousand pesos (PhP500,000.00), or both.

(aa) Violation of Section 31 (b) (ICT-enabled trafficking in persons)-

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

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

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

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

(a b) Violation of Section 32 (a) (ICT-enabled child prostitution) - Violation of Section 5 of the Special Protection of Children Against Abuse, Exploitation and Discrimination Act through ICT - reclusion temporal in its medium period to reclusion perpetua.

(ac) Violation of Section 32 (b) (ICT-enabled child trafficking) - Violation of Section 7 of the Special Protection of Children Against Abuse, Exploitation and Discrimination Act through ICT - reclusion temporal to reclusion perpetua. The penalty shall be imposed in its maximum period when the victim is under twelve (12) years of age.

(ad) Violation of Section 33 (a) (Internet libel) - This shall only give rise to civil liability and the amount shall be commensurate to the damages suffered.

(ae) Violation of Section 33 (b) (Internet hate speech) - This shall only give rise to civil liability and the amount shall be commensurate to the damages suffered.

(af) Violation of Section 33 (c) (Internet child pornography) - Violation of the Anti-Child Pornography Act through ICT - Shall be punished according to the provisions of Section 15 of the Anti-Child Pornography Act of 2009 (RA 9775)

(ag) Violation of Section 33 (d) (Internet child abuse) - Violation of Section 9 of the Special Protection of Children Against Abuse, Exploitation and Discrimination Act through ICT - Shall be punished with imprisonment of prision mayor in its medium period. If the

child used as a performer, subject or seller! distributor is below twelve (12) years of age, the penalty shall b imposed in its maximum period.

(ah) Violation of Section 33 (e) (Internet expression inimical to the public interest) - This shall only give rise to civil liability and the amount shall be commensurate to the damages caused by the Internet expression.

(ai) Violation of Section 34 (b) (Cyberterrorism) - The commission of acts prohibited by the Human Security Act of 2007, as amended, through or using devices, equipment, or physical plants connected to the Internet or to telecommunications networks shall be penalized by the applicable provisions of the Human Security Act of 2007, as amended.

(aj) Violation of Section 34 (c) (ICT-enabled financing of terrorism) - The commission of acts prohibited by the Terrorism Financing Prevention and Suppression Act of 2012, as amended, through or using devices, equipment, or physical plants connected to the Internet or to telecommunications networks shall be penalized by the applicable provisions of the Terrorism Financing Prevention and Suppression Act of 2012, as amended.

(ak) Violation of Section 34 (d) (Cyberespionage) - The commission of acts prohibited by Article 117 of the Revised Penal Code, as amended, through or using devices, equipment, or physical plants connected to the Internet or to telecommunications networks shall be penalized by the applicable provisions of the Revised Penal Code, as amended.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Section 46. Competent law enforcement agencies. -

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

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

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

Section 47. Cybercrime courts. -

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

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

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

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

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

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

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

Section 48. Jurisdiction of cybercrime courts. -

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

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

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

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

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

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

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

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

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

Part 8. Implementing Rules and Regulations.

Section 50. General Implementing Rules and Regulations for the Implementation of the Magna Carta for Philippine Internet Freedom. -

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

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

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

Section 51. Implementing Rules and Regulations for Information and Communications Technology Infrastructure Development. -

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

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

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

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

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

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

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

Section 53. Implementing Rules and Regulations for Information and Communications Technology Education, Training, and Human Resources. -

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

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

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

Section 54. Implementing Rules and Regulations for Information and Communications Technology Research and Development.-

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

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

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

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

(a) The Secretary of National Defense, the Secretary of Interior and Local Government, or their duly authorized and appointed delegates, the Chief of Staff of the Armed Forces of the Philippines (AFP), the commanding general of the unit of the Philippine Air Force tasked with national cyberdefense, the commanding officer of the Intelligence Service, Armed Forces of the Philippines (ISAFP), the commanding officer of the Communication Electronics and Information Systems Service, Armed Forces of the Philippines (CEISSAFP), and the Director-General of the Philippine National Police shall be jointly responsible for the creation of implementing rules and regulations (IRR) of this Act towards ensuring national cyberdefense, cyberintelligence, counter-cyberterrorism, and counter-cyberespionage. The Secretary of Information and Communication Technology shall provide technical advice. The Solicitor-General and the Chairman of the Commission on Human Rights shall participate to ensure that the IRR is not in conflict with this Act, with other laws, with other IRRs of this Act, and with generally accepted principles of international human, civil, and political rights.

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

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

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

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

Section 75. Implementing Rules and Regulations for the Provision of Free WIFI Access- The Secretary of Information and Communication Technology, Secretary of Tourism and the Secretary of Finance shall formulate and promulgate the implementing rules and regulations of this Act towards the designation of selected public areas for free WIFI access.

Section 56. Periodic Review of the Implementing Rules and Regulations of the Magna Carta for Philippine Internet Freedom. -

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

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

Part 9. Final Provisions.

Section 57. Appointment of the Secretory of Information and Communications Technology. - Subject to confirmation by the Commission on Appointments, the President shall appoint the Secretary of Information and Communications Technology within 30 days of the effectivity of this Act.

Section 58. Release of Initial Appropriations. - Subject to government budgetary and audit procedures, the Department of Budget and Management shall release appropriations to the Secretary of Information and Communications Technology for purposes of implementing this Act within 30 days of his appointment.

Section 59. Preparation of Implementing Rules and Regulations. - Within 90 days of the release of initial appropriations, implementing rules and regulations shall have been prepared and approved. The National Cyberdefense and Cybersecurity Plan shall be prepared,

approved, and implemented within 90 days of the approval of the implementing rules and regulations.

Section 60. Compliance of Government ICT Infrastructure and Critical Networks, Data, and Internet Infrastructure. -

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

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

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

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

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

Section 61. Public Information Campaign for the Magna Carta for Philippine Internet Freedom and its Implementing Rules and Regulations. -

(a) The Office of the President, the Presidential Communications Development and Strategic Planning Office or its successor agency, the Philippine Information Agency or its

successor agency, and the Department of Interior and local Government through the information offices of local government units, shall be jointly responsible for information campaigns to ensure nationwide awareness of the Magna Carta for Philippine Internet Freedom and its implementing rules and regulations.

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

Section 62. Initial funding requirements. -

(a) DOJ - The initial funding requirements for the implementation of this Act of the DOJ shall be charged against the current appropriations of the DOJ.

(b) NBI - The initial funding requirements for the implementation of this Act of the NBI shall be charged against the current appropriations of the NBI.

(c) PNP - The initial funding requirements for the implementation of this Act of the PNP shall be charged against the current appropriations of the PNP.

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

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

(f) Other agencies - The initial funding requirements for the implementation of this Act by other agencies shall be charged against the current appropriations of the respective agencies.

Section 63. Succeeding appropriations. - Such sums as may be necessary for the implementation of this Act shall be included in the agencies' yearly budgets under the General Appropriations Act.

Section 64. Separability clause. - If any provision or part hereof is held invalid or unconstitutional, the remainder of the law or the provisions not otherwise affected shall remain valid and subsisting.

Section 65. Repealing clause - Any law, presidential decree or issuance, executive order, letter of instruction, administrative order, rule, or regulation contrary to, or inconsistent with, the provisions of this Act is hereby repealed, modified, or amended accordingly.

Section 66. Effectivity clause. - This Act shall take effect fifteen (15) days after its online publication in the Official Gazette. Within seven (7) days after its online publication, this Act shall be published on (2) newspapers of general circulation.