

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

HOUSE OF REPRESENTATIVES

H.B. No. ~~666~~

Introduced by Representative Herminio Harry L. Roque Jr.

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

EXPLANATORY NOTE

For the better part of the last 20 years, the Internet and information and communication technology (ICT) have increasingly become part of the Filipino way of life. Rare now are the queues before public pay telephones; today, the penetration of mobile phone subscription is pegged by the World Bank at 92%. Instead of handwritten letters and voice tapes, OFWs and their families communicate in real time or in near-real time via Skype, Facebook, Chikka internet-based texting, and email. Students are no longer limited by the size and comprehensiveness of the local library; today, even advanced studies done in developed countries are available to the furthest rural classroom that is equipped with a computer and a broadband connection.

ICT is a practical, strategic agent¹ that is governed by universal ethical rules² and standards,³ and is used to address divisions in culture, education, government openness, receptiveness, and transparency, as well as weaknesses in technical and financial capacity. As

¹ "Utilizing ICT for Sustainable Development in Developing Countries," Rahman.
http://www.academia.edu/1637293/Utilizing_ICT_for_Sustainable_Development_in_Developing_Countries

² "RFC 1087: Ethics and the Internet," Internet Activities Board - Internet Engineering Task Force, 1987.
<https://tools.ietf.org/html/rfc1087>

³ "Tao of the IETF: A Novice's Guide," Internet Engineering Task Force, 2012. <http://www.ietf.org/tao.html>

such, many government officials and agencies have learned that ICT and the Internet are powerful tools to promote their agenda and engage the citizenry. ICT tools and the Internet proved invaluable in disaster management and rescue and relief operations during Ondoy, Pepeng, and Habagat.⁴ Communication through the Internet and social media is the hallmark of the public service of PAGASA (@dost_pagasa), Project Noah (<http://noah.dost.gov.ph/>), and the MMDA (@mmda). The use of ICT, the Internet, and social media can even be argued to have been key to the election of President Benigno S. Aquino III.⁵

ICT has also been a boon to the Philippine economy, even in spite of an annual telecommunications investment of only 0.014 % of the GDP.⁶ Through fast and reliable corporate networks, the BPO, ITO, and other outsourcing industries have contributed USD 11 billion in export revenues, or an estimated 5.4% to the country's GDP in 2011.⁷ The salary scales of the average knowledge worker ranged from P10,000 to P100,000 in 2006,⁸ lessening the pressure for college graduates and professionals to seek employment abroad.

According to a 2009 World Bank study of ICT's impact on economies, for every ten percentage-point increase in high-speed Internet connections there is an increase in economic growth of 1.3 percentage points—contrast this with 0.8 percentage point increase in

⁴ "ANC interview with Communications Undersecretary Manuel L. Quezon III, on engagement through new media platforms," Presidential Communications Development & Strategic Planning Office, 14 August 2012. <http://pcdsपो.gov.ph/2012/08/14/anc-interview-with-communications-undersecretary-manuel-l-quezon-iii-on-engagement-through-new-media-platforms/>

⁵ "Facebook and Twitter — democratising participation in the Philippines," Social Media and Politics: Online Social networking and Political Communication in Asia, Espina-Letargo, 2010. http://www.kas.de/wf/doc/kas_21591-1522-1-30.pdf?110120093225

⁶ "Information and Communication Technology (ICT) Investment in Economically Developing Countries," Negash, 31 December 2006. http://www.academia.edu/400086/Information_and_Communication_Technology ICT_Investment_In_Economically_Developing_Countries

⁷ "After dominating call centers, Philippine IT-BPO seeks world leadership in four more fast growing services," DOST-ICTO, 30 January 2012. http://www.dost.gov.ph/index.php?option=com_content&view=article&id=1096

⁸ "An Input-Output Analysis of the Philippine BPO Industry", Magtibay-Ramos, Estrada, Felipe, 2 October 2007. <http://www.nscb.gov.ph/ncs/10thNCS/papers/invited%20papers/ips-02/ips02-03.pdf>

economic growth per ten percentage point increase in mobile phone subscriptions.⁹ Further economic growth can be expected if the Philippine business environment provides for the healthy growth of Internet and ICT infrastructure and services.

Shortly after the Internet was first used in the country in 1994, legislators have crafted measures to ensure the protection of the public, such as the Electronic Commerce Act (R.A. 8792) and the Data Privacy Act (R.A. 10173). Unfortunately, there remains legislation that confines the Philippines to 20th century capabilities in this 21st century information society. Clearly, laws that have an impact on cyberspace must address the realities of the present and the challenges of the future.

International treaties, agreements, and conventions, such as the UN Convention Against Transnational Organized Crime, the International Convention for the Suppression of the Financing of Terrorism, and the Budapest Convention, have highlighted the need for nation-states to secure their ICT and Internet infrastructure. Reports on the use of ICT as weapons – such as the alleged deployment of the “Stuxnet” worm by the United States against Iran, the alleged hacking of the People’s Republic of China of Google servers, and the recent attack on Middle Eastern oil production infrastructure by the Shamoon virus – have shown the world that ICT can be used as weapons, and have thus shown the need for countries to develop their own cybersecurity and cyberdefense capabilities. This is further complicated by hostile non-state actors and politically-motivated “hacktivists” employing massive botnets as a form of protest or attack, as cheap supercomputing provide even novices the capability to crack tens of thousands of passwords in a few hours. The Philippines has not been spared from such cyberattacks, the most recent being the defacement of the Philippine

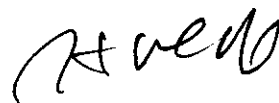
⁹ "Information and Communications for Development 2009: Extending Reach and Increasing Impact," World Bank, 22 July 2009. (permanent URL:<http://go.worldbank.org/NATLOH7HV0>; online reading:<http://issuu.com/world.bank/publications/docs/9780821376058>)

News Agency website by suspected Chinese hackers¹⁰ and a distributed denial-of-service (DDoS) attack on vital government websites and transport, telecommunications, and mass media ICT networks allegedly by Taiwanese hackers.¹¹

The Internet and ICT represent technological advances with the same progressive societal impact as the printing press and the telegraph. Such innovations should be harnessed for the common good, which includes the preservation and promotion of individual rights as guaranteed under the Bill of Rights.

It is time for the establishment of a comprehensive State framework for the administration of the Internet and ICT in the Philippines, a task that should be jointly undertaken by the government and the private sector. Unless this framework is set in place, the temptation looms that the challenges engendered by these new technologies will be addressed in a reactionary, irrational, and haphazard manner that ultimately impedes national progress. This Bill provides for appropriate mechanisms and command structures within the government to address ICT-enabled threats and promote online access and social benefits.

The Magna Carta for Philippine Internet Freedom is envisioned to ensure that the Philippines and its citizens are able to meet the challenges posed by ICT and cyberspace, able to wield it and benefit from it in charting a better future.¹²



HERMINIO HARRY L. ROQUE JR.

¹⁰ "Chinese hackers' deface PNA website," ABS-CBNNews.com, 14 April 2013. <http://www.abs-cbnnews.com/nation/04/14/13/chinese-hackers-deface-pna-website>

¹¹ "Filipino Government Websites Hacked By Taiwanese, And Chinese Netizens Show Surprising Support," International Business Times, Song, 13 May 2013. <http://www.ibtimes.com/filipino-government-websites-hacked-taiwanese-chinese-netizens-show-surprising-support-1254253>

¹² This bill was originally filed during the Fifteenth Congress, Third Regular Session.

Table of Contents

| | Page No. |
|--|-----------------|
| Part 1. General Provisions | |
| Section 1. Short Title | 1 |
| Section 2. Declaration of Policies | 1 |
| Part 2. Definition of Terms | |
| Section 3. Definition of Terms | 3 |
| Part 3. Internet Rights and Freedoms | |
| Section 4. Right to Freedom of Speech and Expression on the Internet | 12 |
| Section 5. Universal Access | 13 |
| Section 6. Right to Privileged Access to and Control of Devices | 15 |
| Section 7. Protection of the Freedom to Innovate and Create Without Permission | 16 |
| Section 8. Right to Privacy of Data | 16 |
| Section 9. Right to Security of Data | 17 |
| Section 10. Protection of Intellectual Property | 18 |
| Section 11. Protection of the Internet as an Open Network | 19 |
| Section 12. Promotion of Network Neutrality | 19 |
| Section 13. Transparency in Governance and Freedom of Information | 20 |
| Part 4. The Department of Information and Communications Technology | |
| Section 14. Department of Information and Communications Technology | 21 |
| Section 15. Strategic Objectives of the DICT | 22 |
| Section 16. Powers and Functions of the DICT | 23 |
| Section 17. Composition of the DICT | 25 |
| Section 18. Secretary of ICT | 26 |
| Section 19. Regional Offices | 27 |

Table of Contents

| | Page No. |
|--|-----------------|
| Section 20. Periodic Performance Review | 28 |
| Section 21. Council of Chief Information Officers | 28 |
| Section 22. National Telecommunication Commission | 28 |
| Section 23. National Data Privacy Commission | 28 |
| Section 24. ICT Legal Affairs Office | 29 |
| Section 25. Telecommunications Office | 29 |
| Section 26. National Information and Communications Technology Institute | 29 |
| Section 27. Freedom of Information and the Official Gazette | 30 |
| Section 28. Compliance with Republic Act No. 6656. | 30 |
| Section 29. Sectoral and Industry Task Forces | 30 |
| Section 30. Structure and Staffing Pattern | 30 |
| Section 31. Magna Carta for Scientists, Engineers, Researchers and other S & T Personnel in the Government | 30 |
| Section 32. Separation from Service | 30 |
| Part 5. Regulations for the Promotion of Internet Rights and Freedoms | |
| Section 33. Declaration of Compliance with Treaty Obligations and International Conventions | 31 |
| Section 34. The State as the Primary Duty-Bearer | 32 |
| Section 35. Duties of the State Agencies and Instrumentalities | 32 |
| Section 36. Amendments to the Public Telecommunications Policy Act of the Philippines | 35 |
| Section 37. Quality of Service and Network Fair Use | 45 |
| Section 38. Amendments to the Intellectual Property Code of the Philippines | 47 |
| Section 39. Content Fair Use | 51 |

Table of Contents

| | Page No. |
|--|----------|
| Section 40. Amendments to the E-Commerce Act | 51 |
| Section 41. Amendments to the Data Privacy Act | 52 |
| Section 42. Repeal of the Cybercrime Prevention Act | 52 |
| Part 6. Cybercrimes and Other Prohibited Acts | |
| Section 43. Network Sabotage | 52 |
| Section 44. Failure to Provide Reasonable Security for Data and Networks | 53 |
| Section 45. Violation of Data Privacy | 54 |
| Section 46. Violation of Data Security | 55 |
| Section 47. Illegal and Arbitrary Seizure | 56 |
| Section 48. Infringement of Intellectual Property Rights | 57 |
| Section 49. Fraud via ICT | 58 |
| Section 50. ICT-Enabled Prostitution and ICT-Enabled Trafficking in Persons | 59 |
| Section 51. ICT-Enabled Child Prostitution and ICT-Enabled Child Trafficking | 60 |
| Section 52. Internet Libel, Hate Speech, Child Pornography, and Other Expression Inimical to the Public Interest | 61 |
| Section 53. Sabotage of Critical Networks and Infrastructure, Acts of Cyberterrorism, and Cyberespionage. | 65 |
| Part 7. National Cybersecurity, Cyberdefense, Counter-Cyberterrorism, and Counter-Cyberespionage | |
| Section 54. Cyberwarfare and National Defense | 68 |
| Section 55. National Cybersecurity and Protection of Government Information and Communications Technology Infrastructure | 68 |
| Section 56. Amendments to the AFP Modernization Act | 69 |
| Section 57. Counter-Cyberterrorism | 71 |
| Section 58. Counter-Cyberespionage | 72 |

Table of Contents

| | Page No. |
|--|----------|
| Part 8. Penalties | |
| Section 59. Applicability of the Penal Code and Other Special Laws | 72 |
| Section 60. Penalties For Specific Violations of the Magna Carta for Philippine Internet Freedom | 72 |
| Section 61. Penalties for Violations of the Magna Carta for Philippine Internet Freedom Affecting Critical Networks and Infrastructure | 80 |
| Section 62. Penalties for Other Violations of the Magna Carta for Philippine Internet Freedom | 80 |
| Section 63. Penalties for Violations of the Magna Carta for Philippine Internet Freedom Committed by a Public Official or Employee | 80 |
| Section 64. 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 Penal Code, and Other Laws | 81 |
| Section 65. Competent Law Enforcement Agencies | 82 |
| Section 66. Cybercrime Courts | 82 |
| Section 67. Jurisdiction of Cybercrime Courts | 83 |
| Section 68. Extraterritorial Application of the Magna Carta for Philippine Internet Freedom | 84 |
| Part 9. Implementing Rules and Regulations | |
| Section 69. Rules and Regulations for the Implementation of the Magna Carta for Philippine Internet Freedom | 84 |
| Section 70. Implementing Rules and Regulations for Information and Communications Technology Infrastructure Development | 85 |
| Section 71. Implementing Rules and Regulations for Cybercrime Law Enforcement | 85 |
| Section 72. Implementing Rules and Regulations for Information and Communications Technology Education, Training, and Human Resources | 85 |
| Section 73. Implementing Rules and Regulations for Information and Communications Technology Research and Development | 85 |

Table of Contents

| | Page No. |
|---|-----------------|
| Section 74. Implementing Rules and Regulations for National Cyberdefense, Cyberintelligence, Counter-Cyberterrorism, and Counter-Cyberespionage | 86 |
| Section 75. Periodic Review of the Implementing Rules and Regulations of the Magna Carta for Philippine Internet Freedom | 87 |
| Part 10. Final Provisions | |
| Section 76. Appointment of the Secretary of Information and Communications Technology | 87 |
| Section 77. Release of Initial Appropriations | 87 |
| Section 78. Preparation of Implementing Rules and Regulations | 87 |
| Section 79. Compliance of Government ICT Infrastructure and Critical Networks, Data, and Internet Infrastructure | 87 |
| Section 80. Public Information Campaign for the Magna Carta for Philippine Internet Freedom and its Implementing Rules and Regulations | 88 |
| Section 81. Initial Funding Requirements | 89 |
| Section 82. Succeeding Appropriations | 90 |
| Section 83. Separability Clause | 90 |
| Section 84. Repealing Clause | 90 |
| Section 85. Effectivity Clause | 90 |

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

HOUSE OF REPRESENTATIVES
H.B. No. 666

Introduced by Representative Herminio Harry L. Roque Jr.

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

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

5 **Part I. General Provisions**

6 SECTION 1. *Short Title.* – This Act shall be known as “The Magna Carta for Philippine
7 Internet Freedom.”

8 SECTION 2. *Declaration of Policies.* – (a) The State affirms that all the rights,
9 guarantees, and privileges provided by the Bill of Rights and the Constitution, as well as those
10 established under general principles of international law and under treaties and conventions to
11 which the Philippines is a signatory, shall govern in the use, development, innovation, and
12 invention of information and communications technology (ICT) and the Internet by the Filipino
13 people.

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

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

19 (d) The growth of the Internet and ICT both depend on and contribute to the growth of

1 the economy, advances in science and technology, and the development of human capital, and
2 encourage democratic discourse and nation-building;

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

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

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

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

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

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

cyberdefense 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.* – Whenever 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), 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.

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

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

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

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

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

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

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

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

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

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

29 (m) Content – Data that can be readily understood by a user immediately upon access,

1 which may include but is not limited to text, pictures, video, or any combination thereof. The
2 word is synonymous to information. Data that is readable and usable only by and between
3 devices, computers, systems or networks, such as traffic data, is not content.

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

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

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

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

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

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

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

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

29 (v) Cyberintelligence – 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 cyberattack and cyberterrorism.

(w) 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.

(x) 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.

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

(z) 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.

(aa) 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

1 information between devices, computers, systems or networks.

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

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

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

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

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

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

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

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

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

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

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

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

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

29 (ai) High-volume connection – A service that provides data connection to the networks

1 and the Internet that allows volumes of uploadable and/or downloadable data larger than what is
2 generally available to the general public.

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

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

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

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

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

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

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

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

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

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

29 (iii) Public information – Any information that is not restricted by virtue of the

1 preceding definitions and can be readily accessed by any interested member of the public.

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

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

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

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

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

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

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

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

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

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

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

29

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

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

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

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

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

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

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

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

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

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

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

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

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

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

27 (i) Processing (Data Privacy Act) – Any operation or any set of operations
28 performed upon personal information including, but not limited to, the collection,
29 recording, organization, storage, updating or modification, retrieval, consultation, use,

1 consolidation, blocking, erasure or destruction of data. (RA 10173)

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

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

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

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

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

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

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

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

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

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

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

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

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

(be) 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.

(bf) 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.

(bg) 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, or nationality.

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

(bi) 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.

(bj) 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.

(bk) 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; and

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

(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, or 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. *Universal Access.* – (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 conviction for any of the following criminal offenses:

(i) The felonies of robbery, theft, estafa, falsification, malversation, and

1 usurpation of authority or official functions, as defined in appropriate penal laws,
2 committed by, through, or using the Internet or information and communications
3 technology;

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

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

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

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

22 Any final judicial relief that seeks to limit or suspend, in whole or in part, one's right to
23 unrestricted access to the Internet, shall be determined in accordance with the appropriate law,
24 including but not limited to the Civil Code and this Act. Any civil action that seeks as a relief, in
25 part or in whole, the limitation or suspension of a person's right to unrestricted access to the
26 Internet, shall be filed exclusively with the Cybercrime Courts.

27 No court shall issue any provisional order suspending the right to unrestricted access to
28 the Internet of any person without prior notice and hearing, and only upon the grounds for the
29 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.

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 interoperability 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.

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

6 SECTION 7. *Protection of the Freedom to Innovate and Create Without Permission.* –

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

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

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

19 SECTION 8. *Right to Privacy of Data.* – (a) The State shall, within its jurisdiction,
20 promote the protection of the privacy of data for all persons.

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

24 (c) Subject to such conditions as provided for in the Data Privacy Act of 2012 (RA
25 10173) and other relevant laws, no person shall access the private data of another person.

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

1 right of privacy.

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

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

8 SECTION 9. *Right to Security of Data.* – (a) The State shall, within its jurisdiction,
9 promote the protection of the security of data for all persons.

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

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

22 (d) No third party granted the right to access the private data or networks of a person by
23 an Internet service provider, telecommunications entity, or other such person providing Internet
24 or data services, shall be given any property rights over the data being accessed, the media where
25 the private data is stored, the equipment through which the network is run or maintained, or the
26 physical plant where the network equipment is housed, beyond the right to access the private
27 data or network, unless otherwise granted such rights by the courts following the appropriate
28 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:

(i) 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.

(h) 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

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

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

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

14 SECTION 11. *Protection of the Internet as an Open Network.* – (a) The State shall,
15 within its jurisdiction, protect and promote the Internet as an open network.

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

25 SECTION 12. *Promotion of Network Neutrality.* – No person or entity shall restrict the
26 flow of data or information on the Internet on the basis of content, nor shall any person institute
27 and employ means or methods to favor the flow of information on the Internet of one class of

1 data or information over another on the basis of content, except:

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

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

6 SECTION 13. *Transparency in Governance and Freedom of Information.* – (a) The State
7 recognizes that the Internet and ICT can facilitate the dissemination of information and the
8 promotion of transparency in governance. Therefore, subject to the provisions of the Data
9 Privacy Act of 2012 (RA10173) and applicable laws on government information classification,
10 the State shall, within practicable and economically reasonable limits, provide for and maintain a
11 system that shall allow the public to view and download public information on plans, policies,
12 programs, documents, and records of government.

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

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

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

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

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

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

1 executive privilege.

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

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

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

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

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

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

23 **Part 4. The Department of Information and Communications Technology**

24 SECTION 14. *Department of Information and Communications Technology*. – (a) There
25 is hereby created the Department of Information and Communications Technology, or DICT.

26 (b) The DICT shall be the primary policy, planning, coordinating, implementing,
27 regulating and administrative entity of the executive branch of the government that will plan,

1 promote and help develop the country's ICT sector and ensure reliable and cost-efficient
2 communications facilities, other multimedia infrastructure and services. The DICT shall likewise
3 be responsible for overseeing the government's integrated and strategic ICT systems and
4 improving the acquisition, utilization and optimization of government's ICT in order to improve
5 the productivity, efficiency, effectiveness and responsiveness of national and local government
6 programs. The DICT shall furthermore be responsible for ensuring the application of ICT to the
7 various processes and functions of the government.

8
9 SECTION 15. *Strategic Objectives of the DICT.* – In fulfilling its mandate, the DICT
10 shall be guided by the following strategic objectives:

11 (a) Ensure the provision of a strategic, reliable, cost-efficient and citizen-centric ICT
12 infrastructure, systems and resources as instruments of nation-building and global
13 competitiveness;

14 (b) Foster a policy environment that will promote a broader market-led ICT and ICT-
15 enabled services sector, a level playing field, partnership between the public and the private
16 sectors, strategic alliance with foreign investors and balanced investments between high-growth
17 and economically depressed areas;

18 (c) Foster and accelerate the convergence of ICT facilities;

19 (d) Ensure universal access and high-speed connectivity at fair and reasonable costs;

20 (e) Ensure the availability and accessibility of ICT services in areas not adequately served
21 by the private sector;

22 (f) Promote and encourage the widespread use, creative development and access to ICT
23 with priority consideration on the requirements for growth of the Philippine ICT industry;

24 (g) Promote and assist the development of local and national content application and
25 services in the area of ICT by sourcing or providing funds and construction assistance for ICT-
26 hubs and/or technical support to local-based providers in these endeavors and in the marketing of
27 the local products to the global community;

28 (h) Establish a strong and effective regulatory and monitoring system that will ensure
29 investor and consumer protection and welfare, and foster a healthy competitive environment;

1 (i) Promote the development of ICT expertise in the country's human capital to enable
2 Filipinos to compete in a fast-evolving information and communication age;

3 (j) Ensure the growth of ICT and ICT-enabled industries;

4 (k) Protect the rights of individuals to privacy and confidentiality of their personal
5 information;

6 (l) Encourage the use of ICT in support of efforts or endeavors for the development and
7 promotion of the country's agriculture, arts and culture, history, education, public health and
8 safety, and other socio-civic purposes;

9 (m) Ensure the security of ICT infrastructure and assets of individuals and businesses;
10 and

11 (n) Empower, through the use of ICT, the disadvantaged segments of the population,
12 including persons with disabilities (PWDs) or who are differently-abled.

13 SECTION 16. *Powers and Functions of the DICT.* – To carry out its mandate, the DICT
14 shall exercise the following powers and functions:

15 (a) Formulate, recommend and/or implement national policies and guidelines in the ICT
16 sector that will promote wider use and development of ICT, and its applications, such as e-
17 commerce, in coordination with the Department of Trade and Industry (DTI), among others;

18 (b) Initiate, harmonize and/or coordinate all ICT plans and initiatives of government
19 agencies to ensure overall consistency and harmony with e-governance objectives, in particular,
20 and national objectives, in general;

21 (c) Represent and negotiate for Philippine interests on matters pertaining to ICT in
22 international bodies;

23 (d) Develop and maintain national ICT development plans and establish and administer
24 comprehensive and integrated programs for ICT with due consideration to advances in
25 convergence and other emerging technologies; and for this purpose, invite any agency,
26 corporation or organization, whether public or private, whose development programs in ICT are
27 integral parts thereof, to participate and assist in the preparation and implementation of various
28 ICT programs for the benefit of the Filipino people;

1 (e) Leverage resources and activities in the various National Government Agencies
2 (NGAs) for database building activity, information and resource sharing and agency networking
3 linkages;

4 (f) Design, implement and ensure the protection of an integrated government information
5 and communications infrastructure development program that will coordinate all relevant
6 government entities, taking into consideration the inventory of existing and projected manpower,
7 plans, programs, proposals, software and hardware, and the installed systems and programs;

8 (g) Provide an integrated framework in order to optimize all government ICT resources
9 and networks and the identification and prioritization of all e-governance systems and
10 applications as provided for in the Government Information Systems Plan and/or the Medium-
11 Term Development Plan (MTDP);

12 (h) Coordinate and support the generation and/or acquisition of all necessary resources
13 and facilities as may be appropriate in and for the development, marketing, growth and
14 competitiveness of the Philippine ICT and ICT-enabled services sector;

15 (i) Develop, implement and improve, in coordination with concerned government
16 agencies and industry associations, the government's ICT application capabilities and determine
17 the personnel qualification and other standards essential to the integrated and effective
18 development and operation of government information and communications infrastructure;

19 (j) Encourage and establish guidelines for private sector funding of ICT projects for
20 government agencies in order to fast-track said projects which provide reasonable cost-recovery
21 mechanisms for the private sector including, but not limited to, build-operate-transfer (BOT) and
22 Public-Private Partnership (PPP) mechanisms;

23 (k) Assess, review and provide direction to ICT research and development programs of
24 the government in coordination with the Department of Science and Technology (DOST) and
25 other institutions concerned;

26 (l) Establish and prescribe rules and regulations for the establishment, operation and
27 maintenance of ICT facilities in areas not adequately served by the private sector, in consultation
28 with the private business sector, local government units (LGUs) and the academe;

29 (m) Administer and enforce all laws, standards, rules and regulations governing ICT;

1 (n) Ensure the protection of ICT-related intellectual property rights in coordination with
2 the Intellectual Property Office (IPO), the Optical Media Board (OMB) and other concerned
3 agencies;

4 (o) Protect the rights of consumer and business users to privacy, security and
5 confidentiality in coordination with concerned agencies;

6 (p) Harmonize, synchronize and coordinate with appropriate agencies all ICT and e-
7 commerce policies, plans and programs;

8 (q) Coordinate with the DTI in the promotion of trade and investment opportunities in
9 ICT and ICT-enabled services;

10 (r) Promote strategic partnership and alliances among and between local and international
11 ICT firms and institutions, research and development, educational and training institutions, and
12 technology providers, developers, and manufacturers to speed up industry growth and enhance
13 global competitiveness, in coordination with concerned agencies;

14 (s) Plan and/or implement such activities as may be appropriate and/or necessary to
15 enhance the competitiveness of Philippine workers, firms and small-to-medium enterprises in the
16 global ICT market and ICT-enabled services market in coordination with concerned agencies;

17 (t) Undertake initiatives to promote ICT and ICT-enabled services in education and
18 training and the development, promotion and application of ICT in education in a manner that is
19 consistent with national goals and objectives, and responsive to the human resources needs of the
20 ICT and ICT-enabled services sector in particular in coordination with concerned agencies;

21 (u) Maximize the use of existing government assets and infrastructure by encouraging
22 private sector investments and partnerships in its operation to achieve total digital inclusion and
23 access to the global information highway; and

24 (v) Formulate guidelines and policies defining the manner of cooperation among Internet
25 service providers, telecommunications companies, and law enforcement agencies during official
26 investigations on violations of existing laws relating to ICT.

27 SECTION 17. *Composition of the DICT.* – (a) The DICT shall be headed by a Secretary
28 to be appointed by the President, subject to confirmation by the Commission on Appointments.

1 The President shall also appoint not more than four (4) Undersecretaries and four (4) Assistant
2 Secretaries.

3 (b) Any person appointed as a Secretary, Undersecretary, or Assistant Secretary of the
4 Department must be a citizen and resident of the Philippines, of good moral character, of proven
5 integrity and with at least seven (7) years of proven competence and expertise in either of the
6 following: information and communications technology, information technology service
7 management, information security management, cybersecurity, data privacy, e-commerce, or
8 human capital development.

9 (c) At least one (1) of the Undersecretaries and one (1) of the Assistant Secretaries shall
10 be a Professional Electronics Engineer as provided for by RA 9292, as amended. At least one (1)
11 of the Undersecretaries and one (1) of the Assistant Secretaries shall be a member of the
12 Philippine Bar. The Assistant Secretaries referred to herein shall be career officers with
13 appropriate eligibilities as prescribed by the Civil Service Commission.

14 SECTION 18. *Secretary of ICT.* – The authority and responsibility for the exercise of the
15 mandate of the DICT and for the discharge of its powers and functions shall be vested in the
16 Secretary of ICT, hereinafter referred to as the SICT, who shall have supervision and control
17 over the DICT. For such purposes, the SICT shall:

18 (a) Provide executive direction and supervision over the entire operations of the DICT
19 and its attached agencies;

20 (b) Establish policies and standards for the effective, efficient and economical operation
21 of the DICT, in accordance with the programs of the government;

22 (c) Rationalize delivery systems necessary for the effective attainment of the objectives
23 of the DICT, including the creation of such offices as may be necessary to ensure the fulfillment
24 of the DICT's mandate, subject to the approval of the Department of Budget and Management
25 (DBM);

26 (d) Review and approve requests for financial and manpower resources of all operating
27 offices of the DICT;

28 (e) Designate and/or appoint all officers and employees of the DICT, except the

Undersecretaries, Assistant Secretaries, Regional and Assistant Regional Directors, and Commissioners and Deputy Commissioners, in accordance with civil service laws, rules and regulations;

(f) Establish coordinative mechanisms to ensure the successful implementation of national ICT policies, initiatives and guidelines in coordination with concerned government units, LGUs, public and private interest groups, including nongovernment organizations (NGOs) and people's organizations (POs);

(g) Advise the President on the promulgation of executive and administrative orders and regulatory and legislative proposals on matters pertaining to ICT development and promotion;

(h) Serve as member of the Government Procurement Policy Board as established by Republic Act No. 9184, otherwise known as the "Government Procurement Reform Act";

(i) Formulate such rules and regulations and exercise such other powers as may be necessary to implement the objectives and purposes of this Act; and

(j) Perform such other tasks as may be provided by law or assigned by the President from time to time.

SECTION 19. *Regional Offices.* – Subject to the concurrence of the Department of Budget and Management and the approval of the President, the DICT may be authorized to establish, operate and maintain a regional office in each of the administrative regions of the country, as the need arises. The regional office shall be headed by a Regional Director, who may be assisted by one (1) Assistant Regional Director. The regional offices shall have, within their respective administrative regions, the following functions:

(a) Implement laws, policies, plans, programs, projects, rules and regulations of the Department;

(b) Provide efficient and effective service to the people;

(c) Coordinate with regional offices of other departments, offices and agencies;

(d) Coordinate with LGUs; and

(e) Perform such other functions as may be provided by law or assigned by the SICT.

1 SECTION 20. *Periodic Performance Review.* – The SICT is hereby required to formulate
2 and enforce a system of measuring and evaluating periodically and objectively the performance
3 of the DICT and to submit the same annually to the President and to appropriate congressional
4 committees.

5 SECTION 21. *Council of Chief Information Officers.* – Every department and agency of
6 the national government or its equivalent office in any constitutional body, state college or
7 university and government-owned and -controlled corporation is hereby directed to appoint or
8 designate at least a third (3rd) ranking official as a Chief Information Officer.

9 The Council of Chief Information Officers shall be composed of eleven (11) members
10 with fixed terms of office, to be appointed by the SICT from sectoral representatives of
11 government departments, constitutional bodies, the academe, LGUs, professional ICT-oriented
12 organizations, and private sector ICT-oriented NGOs. The SICT shall be the Chairperson of the
13 Council.

14 The Council shall serve as a coordinating body to assist the SICT in the establishment of
15 policies, standards, rules and guidelines for ICT initiatives. The Secretary shall convene the
16 Council en banc or by sector at least once every semester within a calendar year.

17 SECTION 22. *National Telecommunication Commission.* – The National
18 Telecommunications Commission or its successor agency shall be attached to the DICT. It shall
19 be responsible for the development, implementation, and enforcement of regulations, standards,
20 instructions, and orders governing ICT infrastructure. The NTC shall be responsible for dispute
21 resolution, and administrative and quasi-judicial proceedings, in the event of civil violations of
22 this Act.

23 SECTION 23. *National Data Privacy Commission.* – The National Data Privacy
24 Commission, as provided for by the Data Privacy Act of 2012 (RA 10173), as amended, shall be
25 attached to the DICT. It shall be responsible for the development, implementation, and
26 enforcement of regulations, standards, instructions, and orders governing data privacy and

1 security. The NDPC shall be responsible for dispute resolution, and administrative and quasi-
2 judicial proceedings, in the event of civil violations of this Act.

3 SECTION 24. *ICT Legal Affairs Office.* – The DICT shall establish an ICT Legal Affairs
4 Office, independent of the NTC and the NDPC, and independent of its other offices. The ICT
5 Legal Affairs office shall be responsible for providing technical assistance to state prosecutors in
6 the event of violations of this Act, and shall be responsible for the filing of cases against persons
7 performing violations of this Act.

8 SECTION 25. *Telecommunications Office.* – The Telecommunications Office or its
9 successor agency shall be attached to the DICT. It shall be responsible for development of
10 national ICT infrastructure primarily in and up to unserved and underserved areas, and the
11 promotion of the use of ICT infrastructure in unserved and underserved areas. The President
12 may, at his discretion, dissolve the Telecommunications Office for reasons of underperformance
13 or nonperformance.

14 SECTION 26. *National Information and Communications Technology Institute.* – The
15 National Computer Center and the National Telecommunications Training Institute shall be
16 combined into the National Information and Communications Technology Institute (NICTI). The
17 NICTI shall be attached to the DICT, and shall be primarily responsible for the development,
18 discretion, and control of information and communications technology as a national resource,
19 such as the acquisition and utilization of computers and related devices, data communications,
20 information systems, software development, and manpower development. It shall be tasked to
21 coordinate all activities related to information technology development in the country, and shall
22 be primarily responsible for the training of government personnel in information and
23 communications technology. The NICTI shall also be tasked to ensure the implementation of an
24 integrated national information and communications technology program.

25 The President may, at his discretion, dissolve the National Information and
26 Communications Technology Institute for reasons of underperformance or nonperformance.

1 SECTION 27. *Freedom of Information and the Official Gazette.* – The DICT and the
2 Official Gazette may establish a clearinghouse for government public information, with the
3 responsibility of publishing online and periodically updating government public information, to
4 promote transparency and citizen engagement through the use of information and
5 communications technology.

6 SECTION 28. *Compliance with Republic Act No. 6656.* – The laws and rules on
7 government reorganization as provided for in Republic Act No. 6656, otherwise known as the
8 Reorganization Law, shall govern the reorganization processes of the DICT.

9 SECTION 29. *Sectoral and Industry Task Forces.* – The DICT may create sectoral and
10 industry task forces, technical working groups, advisory bodies or committees for the furtherance
11 of its objectives. Additional private sector representatives, such as from the academe, the
12 federation of private industries directly involved in ICT, professional ICT-oriented organizations,
13 as well as other NGAs, LGUs and government-owned and -controlled corporations (GOCCs),
14 may be appointed to these working groups. Government IT professionals may also be tapped to
15 partake in the work of the Department through these working groups.

16 SECTION 30. *Structure and Staffing Pattern.* – The DICT shall determine its
17 organizational structure and create new divisions or units as it may deem necessary, subject to
18 the approval of the DBM, and shall appoint officers and employees of the Department in
19 accordance with the Civil Service Law, rules and regulations.

20 SECTION 31. *Magna Carta for Scientists, Engineers, Researchers and other S & T*
21 *Personnel in the Government.* – Employees of the DICT shall be covered by the Magna Carta for
22 Scientists, Engineers, Researchers and other Science & Technology Personnel in the
23 Government (RA 8439).

24 SECTION 32. *Separation from Service.* – (a) Employees separated from the service as a

1 result of the reorganization shall, within ninety (90) days therefrom, receive the retirement
2 benefits to which they may be entitled under existing laws, rules and regulations.

3 (b) Incumbents whose positions are not included in the new position structure and
4 staffing pattern of the DICT or who are not reappointed shall be deemed separated from the
5 service, whether permanent, temporary, contractual or casual employees, and shall, within ninety
6 (90) days therefrom, receive the retirement benefits to which they may be entitled to under
7 existing laws, rules and regulations.

8 **Part 5. Regulations for the Promotion of Internet Rights and Freedoms**

9 SECTION 33. *Declaration of Compliance with Treaty Obligations and International*
10 *Conventions.* – (a) The standards for networks and the Internet, as set by the International
11 Telecommunications Union (ITU), the Internet Engineering Task Force (IETF), the World Wide
12 Web Consortium (WWWC), and the Internet Corporation for Assigned Numbers and Names
13 (ICANN), and their successors-in-interest are hereby adopted. No agency or instrumentality of
14 the State shall issue rules and regulations contrary to these.

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

18 (c) The State reaffirms its compliance to the treaties and international conventions to
19 which it is a signatory, to wit, the International Covenant on Civil and Political Rights (ICCPR),
20 the International Covenant on Economic, Social, and Cultural Rights (ICESCR), the Convention
21 on the Rights of the Child (CRC), the Convention on the Elimination of All Forms of Racial
22 Discrimination (ICERD), the Convention on the Elimination of All Forms of Discrimination
23 Against Women (CEDAW), the Convention on the Rights of Persons with Disabilities (CRPD),
24 the United Nations Convention against Transnational Organized Crime, the United Nations
25 Convention against Corruption, the Geneva Convention, the United Nations Convention on
26 Certain Conventional Weapons, the Rome Statute of the International Criminal Court, the
27 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.

(d) 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 34. *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 35. *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.

1 (d) Information and Communications Technology Infrastructure Development. –

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

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

17 (iii) The procurement by the national government or by local governments of
18 ICT-related goods and services which will not be implemented under Republic Act No.
19 6957, as amended by Republic Act No. 7718, shall be governed by Republic Act No.
20 9184.

21 (iv) The development and operation of information and communications
22 technology infrastructure and facilities is hereby declared as a preferred area of
23 investment and shall be included in the annual Investment Priority Plan issued in
24 accordance with the Omnibus Investments Code. Subject to the contrary factual
25 determination of the Board of Investments, an entity involved in the development and
26 operation of information and communications technology infrastructure and facilities is
27 presumed to be entitled to register as a registered enterprise under the Investment
28 Priorities Plan; *Provided*, that an enterprise that proposes to operate a public utility or
29 public service shall be subject to the equity requirements imposed by the Constitution and

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

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

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

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

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

27 (g) Intellectual Property Rights Protection in Cyberspace. – Subject to provisions of this
28 Act and other relevant laws, the Intellectual Property Office shall, within Philippine jurisdiction,
29 be primarily responsible for the protection of intellectual property rights in cyberspace. As

1 official registrar and repository of copies of published works, the National Library and the
2 National Archives shall assist the Intellectual Property Office in the protection of copyright.

3 SECTION 36. *Amendments to the Public Telecommunications Policy Act of the*
4 *Philippines.* – (a) Jurisdiction over the provision and regulation of Internet and information and
5 communications technology services shall be vested with the National Telecommunications
6 Commission, in accordance with the succeeding provisions.

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

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

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

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

24 c) Mandate a fair and reasonable interconnection of facilities of
25 authorized public network operators and other providers of telecommunications,
26 **NETWORK, AND INTERNET** services through appropriate modalities of
27 interconnection and at a reasonable and fair level of charges, which make
28 provision for the cross subsidy to unprofitable local exchange service areas so as

1 to promote telephone [density], **MOBILE PHONE, NETWORK, AND**
2 **BROADBAND DENSITY** and provide the most extensive access to basic
3 telecommunications, **NETWORK, AND INTERNET** services available at
4 affordable rates to the public;

5 xxx xxx xxx

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

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

17 *"Section 6. Responsibilities of and Limitations to Department Powers. -*

18 The Department of [Transportation and Communications (DOTC)]
19 **INFORMATION AND COMMUNICATIONS TECHNOLOGY (DICT)** shall
20 not exercise any power which will tend to influence or effect a review or a
21 modification of the Commission's quasi-judicial functions.

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

24 xxx xxx xxx

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

29 d) the operation of a national consultative forum to facilitate interaction

1 amongst the [telecommunications industries] **INFORMATION,**
2 **COMMUNICATIONS, NETWORK, AND INTERNET INDUSTRIES,**
3 **USER GROUPS,** academic and research institutions in the airing and resolution
4 of important issues in the field of [communications]
5 **TELECOMMUNICATIONS AND THE INTERNET. xxx”**

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

8 ***“SECTION 10A. LOCAL INTERNET SERVICE PROVIDER. – A***
9 **LOCAL INTERNET SERVICE PROVIDER SHALL:**

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

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

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

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

29 **PROVIDED THAT THE SERVICE IT PROVIDES IS SOLELY**

1 DEPENDENT ON EXISTING NETWORKS BEING OPERATED AND
2 MAINTAINED BY AT LEAST ONE OTHER TELECOMMUNICATIONS
3 ENTITY, A LOCAL INTERNET SERVICE PROVIDER NEED NOT
4 SECURE A FRANCHISE.

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

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

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

25 (A) IT SHALL INTERCONNECT WITH ALL OTHER INTERNET
26 EXCHANGES IN THE SAME CATEGORY AND WITH ALL LOCAL
27 INTERNET SERVICE PROVIDERS AND OTHER
28 TELECOMMUNICATIONS ENTITIES, UPON APPLICATION AND
29 WITHIN A REASONABLE TIME PERIOD, AND UNDER FAIR AND

1 REASONABLE LEVEL CHARGES, IN ORDER THAT INTERNET AND
2 NETWORK SERVICES ARE MADE POSSIBLE; AND

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

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

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

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

28 (B) IT SHALL HAVE THE RIGHT TO ESTABLISH AND
29 OPERATE ITS OWN NETWORK FACILITIES THROUGH WHICH

1 INTERNATIONAL NETWORKS OR INTERNATIONAL GATEWAY
2 FACILITIES SHALL BE ABLE TO COURSE THEIR MESSAGES OR
3 SIGNALS.

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

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

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

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

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

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

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

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

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

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

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

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

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

8 **THE PROVISION OF HIGH-SPEED OR HIGH-VOLUME**
9 **INTERNET CONNECTION OR DATA TRANSMISSION SERVICES AS A**
10 **SERVICE SEPARATE FROM NORMAL INTERNET CONNECTION OR**
11 **DATA TRANSMISSION SERVICES SHALL NOT BE CLASSED AS A**
12 **VALUE-ADDED SERVICE.”**

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

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

22 **UNLESS DESIGNED AND MANUFACTURED AS SUCH**
23 **WITHOUT NEED FOR A SPECIAL REQUEST BY A**
24 **TELECOMMUNICATIONS ENTITY, NO CUSTOMER PREMISES**
25 **EQUIPMENT SHALL BE RESTRICTED FROM INTERCONNECTING**
26 **TO A NETWORK OR TO THE INTERNET, OR INTEROPERABILITY**
27 **WITH OTHER CUSTOMER PREMISES EQUIPMENT, NETWORK**
28 **EQUIPMENT, DATA STORAGE EQUIPMENT, OR OTHER DEVICES**
29 **OR EQUIPMENT THAT MAY BE NORMALLY INTERCONNECTED**

1 WITH OR MAY NORMALLY ENJOY INTEROPERABILITY WITH, AS
2 APPLICABLE; PROVIDED, HOWEVER, THAT IN THE COURSE OF
3 NORMAL OPERATIONS SUCH INTERCONNECTION OR
4 INTEROPERABILITY SHALL NOT COMPROMISE DATA OR
5 NETWORK PRIVACY OR SECURITY.”

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

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

11 xxx xxx xxx

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

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

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

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

1 MESSAGE SERVICE (MMS) MESSAGES, OR EMAIL, and shall keep a
2 record of all [written or phoned-in] complaints received and the actions taken to
3 address these complaints.

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

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

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

21 (2) THE UTILITY HAS EVIDENCE THAT THE NON-
22 COMPLIANCE HAS NOT RECURRED, IS NOT RECURRING, NOR
23 WILL RECUR IN THE FUTURE; OR THE UTILITY HAS EVIDENCE
24 THAT THE NONCOMPLIANCE WAS DUE TO FACTORS BEYOND ITS
25 CONTROL; OR THE UTILITY HAS PROVIDED IMMEDIATE REFUND
26 OR REBATE TO THE USER UPON DETECTION OF THE
27 NONCOMPLIANCE; OR THE UTILITY HAS EVIDENCE THAT IT HAS
28 EXERTED ITS BEST EFFORTS TO RESOLVE THE NONCOMPLIANCE
29 AND RESTORE THE SERVICE TO THE LEVEL AGREED BETWEEN

1 THE UTILITY AND THE USER WITHIN SEVEN (7) DAYS OF THE
2 REQUEST FOR IMMEDIATE TERMINATION; AND THE UTILITY
3 SHALL COMPLY WITH IMMEDIATE TERMINATION OF SERVICE,
4 WITHOUT THE IMPOSITION OF FEES OR PENALTIES, AND REFUND
5 ANY FEES OR CHARGES ALREADY PAID BY THE USER WITHOUT
6 NEED FOR DEMAND SHOULD THE SERVICE NOT BE RESTORED
7 WITHIN THE SEVEN (7) DAY PERIOD, WITHIN THREE (3) DAYS
8 AFTER THE TERMINATION OF SERVICE.

9 SUBJECT TO STANDARDS SET BY THE COMMISSION,
10 PENALTIES MAY BE IMPOSED ON A UTILITY THAT IS UNABLE TO
11 COMPLY WITH PRECEDING PARAGRAPHS (B) AND (C). THE
12 COMMISSION MAY IMPOSE ADDITIONAL PENALTIES IF THE
13 UTILITY DOES NOT REFUND ANY DEPOSITS, FEES, OR CHARGES
14 ALREADY PAID BY THE USER WITHOUT NEED FOR DEMAND
15 WITHIN THREE (3) DAYS AFTER THE DEADLINE AGREED UPON
16 BETWEEN THE USER AND THE UTILITY.”

17 SECTION 37. *Quality of Service and Network Fair Use.* – (a) No Internet service
18 provider, Internet exchange, Internet data center, Internet gateway facility, telecommunications
19 entity, or person providing Internet connection, network, or data transmission services shall:

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

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

27 (iii) Block, impair, or discriminate against, or to interfere with the ability of any
28 person to use a network service to access, to use, to send, to receive, or to offer lawful

1 content, applications, or services over the Internet;

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

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

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

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

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

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

20 (ii) To give priority to emergency communications;

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

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

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

26 (c) An Internet service provider, Internet exchange, Internet data center, Internet gateway
27 facility, telecommunications entity, or person providing Internet connection, network, or data
28 transmission services may provide for different levels of availability, uptime, or other service
29 quality standards set by the National Telecommunications Commission for services using

1 prepaid, postpaid, or other means of payment; *Provided*, that minimum levels of availability,
2 uptime, and other service quality standards set by the Commission shall not be different between
3 services using prepaid, postpaid, or other means of payment.

4 SECTION 38. *Amendments to the Intellectual Property Code of the Philippines.* –

5 (a) The Intellectual Property Code of the Philippines (Republic Act No. 8293), Part IV,
6 Chapter II, Section 172 is hereby amended to read:

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

11 xxx xxx xxx

12 (n) **CODE, SCRIPTS, COMPUTER PROGRAMS, SOFTWARE**
13 **APPLICATIONS, AND OTHER SIMILAR WORK, WHETHER**
14 **EXECUTABLE IN WHOLE OR AS PART OF ANOTHER CODE,**
15 **SCRIPT, computer programs, SOFTWARE APPLICATION OR OTHER**
16 **SIMILAR WORK;**

17 xxx xxx xxx

18 172.2. Works are protected by the sole fact of their creation, irrespective
19 of their mode or form of expression **OR PUBLICATION**, as well as of their
20 content, quality and purpose.”

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

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

27 **177.1 COPYRIGHT –SUBJECT TO THE PROVISIONS OF**
28 **CHAPTER VIII, ECONOMIC RIGHTS UNDER THIS SECTION SHALL**

1 CONSIST OF THE EXCLUSIVE RIGHT TO CARRY OUT, AUTHORIZE
2 OR PREVENT THE FOLLOWING ACTS:

3 xxx xxx xxx

4 **177.2. COPYLEFT – IS THE EXERCISE OF ECONOMIC RIGHTS**
5 **OVER ORIGINAL AND DERIVATIVE WORKS, INCLUDING FREE**
6 **AND OPEN-SOURCE SOFTWARE, WHERE THE AUTHOR**
7 **IRREVOCABLY ASSIGNS TO THE PUBLIC, EITHER PARTIALLY OR**
8 **FULLY, ONE OR SEVERAL RIGHTS IN COMBINATION, THE RIGHT**
9 **TO USE, MODIFY, EXTEND, OR REDISTRIBUTE THE ORIGINAL**
10 **WORK. UNDER COPYLEFT, ANY AND ALL WORKS DERIVED FROM**
11 **THE ORIGINAL WORK SHALL BE COVERED BY THE SAME**
12 **LICENSE AS THE ORIGINAL WORK. DECLARATION OF A**
13 **COPYLEFT LICENSE SHALL BE SUFFICIENT IF A STATEMENT OF**
14 **THE APPLICABLE COPYLEFT LICENSE IS STIPULATED ON A COPY**
15 **OF THE WORK AS PUBLISHED.**

16 **177.3 FREE OR PUBLIC – IS THE EXERCISE OF ECONOMIC**
17 **RIGHTS OVER ORIGINAL AND DERIVATIVE WORKS WHERE THE**
18 **AUTHOR IRREVOCABLY ASSIGNS TO THE PUBLIC ALL THE**
19 **RIGHTS TO USE, MODIFY, EXTEND, OR REDISTRIBUTE THE**
20 **ORIGINAL WORK WITHOUT ANY RESTRICTIONS, OR WHERE THE**
21 **AUTHOR IRREVOCABLY DECLARES THE WORK TO BE PUBLIC**
22 **DOMAIN UNDER SECTIONS 175 AND 176 OF THIS CODE. THE**
23 **REDISTRIBUTION OF ANY MODIFIED OR DERIVATIVE WORK**
24 **SHALL NOT BE REQUIRED TO ADOPT FREE OR PUBLIC RIGHT.**
25 **ADOPTION OR DECLARATION OF THIS RIGHT SHALL BE**
26 **SUFFICIENT IF A STATEMENT TO THE EFFECT IS STIPULATED ON**
27 **A COPY OF THE WORK AS PUBLISHED.**

28 **177.4 EXCEPT WITH RESPECT TO ECONOMIC RIGHTS**
29 **UNDER COPYLEFT, THE AUTHOR OR COPYRIGHT OWNER SHALL**

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

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

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

13 xxx xxx xxx

14 180.3. The submission of a literary, photographic or artistic work to a
15 newspaper, magazine or periodical for publication, shall constitute only a license
16 to make a single publication unless a greater right is expressly granted. **IN THE**
17 **CASE OF POSTING TO A WEBSITE OR AN ONLINE VERSION OF A**
18 **NEWSPAPER, MAGAZINE, OR PERIODICAL, ENABLING ACCESS TO**
19 **THE WHOLE OR PORTION OF THE WORK VIA AUTOMATIC**
20 **CONTENT SYNDICATION OR SEARCH RESULTS SHALL NOT**
21 **CONSTITUTE VIOLATION OF THE LICENSE UNLESS THE**
22 **CONTRARY IS EXPRESSLY PROVIDED IN A WRITTEN AGREEMENT**
23 **BETWEEN COPYRIGHT OWNER AND PUBLISHER/HOST/SERVICE**
24 **PROVIDER.** If two (2) or more persons jointly own a copyright or any part
25 thereof, neither of the owners shall be entitled to grant licenses without the prior
26 written consent of the other owner or owners. xxx”

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

29 “Section 182. *Filing of Assignment or License OF COPYRIGHT.* – An

1 assignment or exclusive license may be filed in duplicate with the National
2 Library upon payment of the prescribed fee for registration in books and records
3 kept for the purpose. Upon recording, a copy of the instrument shall be returned to
4 the sender with a notation of the fact of record. Notice of the record shall be
5 published in the IPO Gazette. xxx”

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

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

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

16 xxx xxx xxx

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

19 xxx xxx xxx

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

29 (f) The Intellectual Property Code of the Philippines, Part II, Chapter IX, Section 192

1 shall be amended to read:

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

11 SECTION 39. *Content Fair Use.* – (a) Subject to the provisions of the Intellectual
12 Property Code of the Philippines, as amended, and this Act and other relevant laws, the viewing
13 of online content on any computer, device, or equipment shall be considered fair use.

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

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

24

25 SECTION 40. *Amendments to the E-Commerce Act.* – Subject to the provisions of this
26 Act, paragraphs (a) and (b) of Section 33 of the Electronic Commerce Act of 2000 (RA 8792) are
27 hereby repealed.

SECTION 41. *Amendments to the Data Privacy Act.* – (a) Subject to the provisions of this Act, the Data Privacy Act of 2012 (RA 10173), Section 7 is hereby amended 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:
xxx”

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

Part 6. Cybercrimes and Other Prohibited Acts

SECTION 43. *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 or 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 44. *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

1 maintained, or the physical plant where the data or network equipment is housed shall be
2 presumed to be the result of criminal negligence, except upon a final ruling from the courts,
3 issued following due notice and hearing.

4 SECTION 45. *Violation of Data Privacy.* – (a) Unauthorized access. – It shall be
5 unlawful for any person to intentionally access data, networks, storage media where data is
6 stored, equipment through which networks are run or maintained, the physical plant where the
7 data or network equipment is housed, without authority granted by the Internet service provider,
8 telecommunications entity, or other such person providing Internet or data services having
9 possession or control of the data or network, or to intentionally access intellectual property
10 published on the Internet or on other networks without the consent of the person having
11 ownership, possession, or control of the intellectual property, or without legal grounds, even if
12 access is performed without malice.

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

21 (c) Unauthorized authorization or granting of privileges. – It shall be unlawful for any
22 person to intentionally provide a third party authorization or privileges to access or modify data,
23 networks, storage media where data is stored, equipment through which networks are run or
24 maintained, the physical plant where the data or network equipment is housed, without authority
25 granted by the Internet service provider, telecommunications entity, or other such person
26 providing Internet or data services having possession or control of the data or network, or to
27 intentionally provide a third party authorization to access or modify intellectual property
28 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 46. *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 47. *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

1 seizure, possession, or control.

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

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

16 SECTION 48. *Infringement of Intellectual Property Rights.* –

17 (a) Copyright infringement. –

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

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

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

27 (iv) Subject to the Intellectual Property Code of the Philippines and the laws
28 governing fair use, it shall be unlawful for any person to reverse-engineer any whole or

1 part of any computer program, software, code, or script, whether or not executable, that is
2 the subject of a copyright, and that he does not have any property rights over, or does not
3 acknowledge and comply with the terms of copyright or license governing the intellectual
4 property rights enjoyed by the computer program being reverse-engineered.

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

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

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

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

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

23 SECTION 49. *Fraud via ICT.* – It shall be unlawful for any person who knowingly by
24 means of a device, equipment, or physical plant connected to the Internet, to telecommunications
25 networks, a network of a government agency, the government network, a private network or any
26 protected computer or device, or in connivance with a third party with access to the same, shall
27 use the Internet, telecommunications networks, private networks, or government networks for the
28 purpose of deceiving or defrauding another of money, goods, or property, or to do the same by or

1 through exceeding authorized access.

2 SECTION 50. *ICT-Enabled Prostitution and ICT-Enabled Trafficking in Persons.* – (a)

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

10 (b) ICT-Enabled Trafficking in Persons. –

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

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

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

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

23 xxx xxx xxx

24 (c) To advertise, publish, print, broadcast or distribute, or cause the
25 advertisement, publication, printing, broadcasting or distribution by any means,
26 including the use of information **AND COMMUNICATIONS** technology and
27 the Internet, of any brochure, flyer, or any propaganda material that promotes
28 trafficking in persons, **OR TO KNOWINGLY, WILLFULLY AND**

1 INTENTIONALLY PROVIDE DEVICES, EQUIPMENT, OR PHYSICAL
2 PLANTS CONNECTED TO THE INTERNET OR TO
3 TELECOMMUNICATIONS NETWORKS, WITH THE PRIMARY
4 PURPOSE OF PROMOTING TRAFFICKING IN PERSONS; xxx.”

5 SECTION 51. *ICT-Enabled Child Prostitution and ICT-Enabled Child Trafficking.* –

6 (a) ICT-Enabled Child Prostitution. -

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

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

13 “Section 5. *Child Prostitution and Other Sexual Abuse.* –

14 xxx xxx xxx

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

24 xxx xxx xxx

25 (c) Those who derive profit or advantage therefrom, whether as manager
26 or owner of the establishment where the prostitution takes place, or of the sauna,
27 disco, bar, resort, place of entertainment or establishment serving as a cover or
28 which engages in prostitution in addition to the activity for which the license has

1 been issued to said establishment; **OR THOSE WHO DERIVE PROFIT OR**
2 **ADVANTAGE THEREFROM, WHETHER AS AUTHOR,**
3 **ADMINISTRATOR, OR AUTHORIZED USER OF THE DEVICE,**
4 **EQUIPMENT, NETWORK, PHYSICAL PLANT, OR WEBSITE**
5 **CONNECTED TO THE INTERNET OR TO TELECOMMUNICATIONS**
6 **NETWORKS CREATED OR ESTABLISHED WITH THE PURPOSE OF**
7 **INDUCING A PERSON TO ENGAGE IN CHILD PROSTITUTION. xxx”**

8 (b) ICT-Enabled Child Trafficking. –

9 (i) The Special Protection of Children Against Abuse, Exploitation and
10 Discrimination Act, Section 7 shall be amended to read:

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

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

27 SECTION 52. *Internet Libel, Hate Speech, Child Pornography, and Other Expression*

1 *Inimical to the Public Interest.* –

2 (a) Internet libel. –

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

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

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

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

18 (v) Exceptions to internet libel. – The following acts shall not constitute internet
19 libel:

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

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

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

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

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

1 entities provide;

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

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

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

12 (b) Internet hate speech. –

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

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

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

26 (c) Internet child pornography. –

27 (i) The performance of acts prohibited by Sections 4 and 5 of R.A. No. 9775, or
28 the Anti-Child Pornography Act of 2009, by means of a device, storage medium, network
29 equipment, or physical plant connected to the Internet or to telecommunications networks

1 shall be deemed unlawful.

2 (ii) The commission of acts prohibited by the Anti-Child Pornography Act of
3 2009 through or using devices, equipment, or physical plants connected to the Internet or
4 to telecommunications networks shall be penalized by the applicable provisions of the
5 Anti-Child Pornography Act of 2009.

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

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

17 (f) For film distributors, theaters, **INTERNET SERVICE PROVIDERS,**
18 and telecommunication companies, by themselves or in cooperation with other
19 entities, to distribute any form of child pornography; xxx”

20 (d) Internet child abuse. –

21 (i) The performance of acts prohibited by Section 9 of the Special Protection of
22 Children Against Abuse, Exploitation and Discrimination Act, by means of a device,
23 storage medium, network equipment, or physical plant connected to the Internet or to
24 telecommunications networks shall be deemed unlawful.

25 (ii) The commission of acts prohibited by the Special Protection of Children
26 Against Abuse, Exploitation and Discrimination Act, through or using devices,
27 equipment, or physical plants connected to the Internet or to telecommunications
28 networks shall be penalized by the applicable provisions of the Special Protection of
29 Children Against Abuse, Exploitation and Discrimination Act.

(iii) The Special Protection of Children Against Abuse, Exploitation and Discrimination Act, Section 9 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 53. *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); 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,

1 storage medium, network equipment, or physical plant connected to the Internet or to
2 telecommunications networks shall be deemed unlawful.

3 (ii) The commission of acts prohibited by the Human Security Act of 2007,
4 through or using devices, equipment, or physical plants connected to the Internet or to
5 telecommunications networks shall be penalized by the applicable provisions of the
6 Human Security Act of 2007.

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

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

10 xxx xxx xxx

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

14 **7. SECTION 25 (NETWORK SABOTAGE), SECTION 27**
15 **(VIOLATION OF DATA PRIVACY), AND SECTION 28 (VIOLATION OF**
16 **DATA SECURITY) OF THE MAGNA CARTA FOR PHILIPPINE**
17 **INTERNET FREEDOM COMMITTED AGAINST CRITICAL DATA,**
18 **NETWORK, INTERNET, OR TELECOMMUNICATIONS**
19 **INFRASTRUCTURE, WHETHER PUBLICLY OR PRIVATELY OWNED,**
20 **xxx”**

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

22 (i) The commission of acts prohibited by the Terrorism Financing Prevention and
23 Suppression Act of 2012, through or using devices, equipment, or physical plants
24 connected to the Internet or to telecommunications networks shall be penalized by the
25 applicable provisions of the Terrorism Financing Prevention and Suppression Act of
26 2012.

27 (ii) The Terrorism Financing Prevention and Suppression Act of 2012, Section 4
28 shall be amended to read:

29 *“Section 4. Financing of Terrorism. –*

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. – The Penal Code, Article 117 shall be amended to read:

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

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

1 **OR INFORMATION CLASSIFIED BY LAW AS STATE SECRETS; OR**

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

6 **Part 7. National Cybersecurity, Cyberdefense, Counter-Cyberterrorism, and**
7 **Counter-Cyberespionage**

8 SECTION 54. *Cyberwarfare and National Defense.* – (a) It shall be unlawful for any
9 person, or military or civilian agency, or instrumentality of the State to initiate a cyberattack
10 against any foreign nation, except in the event of a declaration of a state of war with the foreign
11 nation.

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

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

22 SECTION 55. *National Cybersecurity and Protection of Government Information and*
23 *Communications Technology Infrastructure.* – (a) The Secretary of National Defense shall
24 assist the President in the protection and conduct of the national cybersecurity, and the conduct
25 of cyberdefense and the protection of national government information and communications
26 technology infrastructure.

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

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

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

16 SECTION 56. *Amendments to the AFP Modernization Act.* – The Armed Forces of
17 the Philippines Modernization Act (RA 7898), Section 5 shall be amended to read:

18 “Section 5. *Development of AFP Capabilities.* – The AFP modernization
19 program shall be geared towards the development of the following defense
20 capabilities:

21 xxx xxx xxx

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

1 (1) DETECT, IDENTIFY, INTERCEPT AND ENGAGE, IF
2 NECESSARY, ANY ATTEMPTED OR ACTUAL PENETRATION OR
3 CYBERATTACK OF PHILIPPINE GOVERNMENT INFORMATION
4 AND COMMUNICATIONS TECHNOLOGY INFRASTRUCTURE, AS
5 WELL AS CRITICAL INFORMATION AND COMMUNICATIONS
6 TECHNOLOGY INFRASTRUCTURE WITHIN PHILIPPINE
7 JURISDICTION;

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

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

13 (E) DEVELOPMENT OF CYBERINTELLIGENCE CAPABILITY.
14 – THE INTELLIGENCE SERVICE OF THE ARMED FORCES OF THE
15 PHILIPPINES (ISAFP) OR ITS SUCCESSOR SERVICE, SHALL
16 DEVELOP ITS CYBERINTELLIGENCE CAPABILITY. THE
17 CYBERINTELLIGENCE CAPABILITY SHALL ENABLE THE AFP TO:

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

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

28 (3) PROVIDE, AND IF PRACTICABLE, INVENT OR INNOVATE,
29 THROUGH FILIPINO SKILLS AND TECHNOLOGY, ITS OWN

1 **REQUIREMENTS FOR NATIONAL CYBERINTELLIGENCE.**

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

11 SECTION 57. *Counter-Cyberterrorism.* – (a) The Philippine National Police, supported
12 by applicable military, law enforcement, and government services, offices, and agencies, shall be
13 the lead law enforcement agency responsible for plans, policies, programs, measures, and
14 mechanisms to detect, identify, and prevent cyberterrorist attacks on Philippine government
15 information and communications technology infrastructure, as well as publicly- and privately-
16 owned information and communications technology infrastructure within Philippine jurisdiction,
17 and the detection, identification, pursuit, apprehension, and the gathering of evidence leading to
18 the conviction of persons committing cyberterrorism.

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

25 (c) Subject to the provisions of an existing treaty to which the Philippines is a signatory
26 and to any contrary provision of any law of preferential application, and subject to the
27 concurrence of the Secretary of Justice and the Secretary of Foreign Affairs, the Director of the
28 National Bureau of Investigation may cooperate with or request the cooperation of foreign or

1 international law enforcement agencies in the detection, identification, pursuit, apprehension, and
2 the gathering of evidence leading to the conviction of persons who, although physically outside
3 the territorial limits of the Philippines, have committed or are attempting to commit acts of
4 cyberterrorism within Philippine jurisdiction.

5 SECTION 58. *Counter-Cyberespionage.* – (a) The National Intelligence Coordinating
6 Agency, supported by applicable military, law enforcement, and government services, offices,
7 and agencies, shall be the lead agency responsible for plans, policies, programs, measures, and
8 mechanisms to detect, identify, and prevent cyberespionage attempts and incidents.

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

13 **Part 8. Penalties**

14 SECTION 59. *Applicability of the Penal Code and other special laws.* – Nomenclature
15 notwithstanding, the provisions of Book I of the Penal Code shall apply suppletorily to the
16 provisions of this Act, whenever applicable.

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

18 SECTION 60. *Penalties For Specific Violations of The Magna Carta for Philippine*
19 *Internet Freedom.* – The following penalties shall be imposed for specific violations of this Act:

20 (a) Violation of Section 42 (a) (Direct network sabotage) shall be punished with
21 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
22 (P500,000.00), or both.

23 (b) Violation of Section 42 (b) (Indirect network sabotage) shall be punished with
24 imprisonment of *prision correccional* in its medium period or a fine of not more than three
25 hundred thousand pesos (P300,000.00), or both.

1 (c) Violation of Section 43 (a) (Failure to provide security) shall be punished with
2 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
3 (P500,000.00), or both.

4 (d) Violation of Section 43 (b) (Negligent failure to provide security) shall be punished
5 with imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
6 pesos (P500,000.00), or both.

7 (e) Violation of Section 44 (a) (Unauthorized access) shall be punished with
8 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
9 hundred thousand pesos (P500,000.00) but not more than Two million pesos (P2,000,000.00).

10 (f) Violation of Section 44 (b) (Unauthorized modification) shall be punished with
11 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
12 hundred thousand pesos (P500,000.00) but not more than Two million pesos (P2,000,000.00).

13 (g) Violation of Section 44 (c) (Unauthorized granting of privileges) shall be punished
14 with imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
15 hundred thousand pesos (P500,000.00) but not more than Two million pesos (P2,000,000.00).

16 (h) Violation of Section 44 (d) (Unauthorized disclosure) shall be punished with
17 imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five
18 hundred thousand pesos (P500,000.00) but not more than Two million pesos (P2,000,000.00).

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

20 (i) Violation of Section 25 (a) of the Data Privacy Act (Unauthorized Processing
21 of Personal Information) through ICT shall be punished with imprisonment ranging from
22 one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos
23 (P500,000.00) but not more than Two million pesos (P2,000,000.00).

24 (ii) Violation of Section 25 (b) of the Data Privacy Act (Unauthorized Processing
25 of Sensitive Personal Information) through ICT shall be punished with imprisonment
26 ranging from three (3) years to six (6) years and a fine of not less than Five hundred
27 thousand pesos (P500,000.00) but not more than Four million pesos (P4,000,000.00).

28 (iii) Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal
29 Information Due to Negligence) through ICT shall be punished with imprisonment

1 ranging from one (1) year to three (3) years and a fine of not less than Five hundred
2 thousand pesos (P500,000.00) but not more than Two million pesos (P2,000,000.00).

3 (iv) Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
4 Personal Information Due to Negligence) through ICT shall be punished with
5 imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five
6 hundred thousand pesos (P500,000.00) but not more than Four million pesos
7 (P4,000,000.00).

8 (v) Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of
9 Personal Information) through ICT shall be punished with imprisonment ranging from six
10 (6) months to two (2) years and a fine of not less than One hundred thousand pesos
11 (P100,000.00) but not more than Five hundred thousand pesos (P500,000.00).

12 (vi) Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of
13 Sensitive Personal Information) through ICT shall be punished with imprisonment
14 ranging from one (1) year to three (3) years and a fine of not less than One hundred
15 thousand pesos (P100,000.00) but not more than One million pesos (P1,000,000.00).

16 (vii) Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal
17 Information for Unauthorized Purposes) through ICT shall be punished with
18 imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of
19 not less than Five hundred thousand pesos (P500,000.00) but not more than One million
20 pesos (P1,000,000.00).

21 (viii) Violation of Section 28 (b) of the Data Privacy Act (Processing of Sensitive
22 Personal Information for Unauthorized Purposes) through ICT shall be punished with
23 imprisonment ranging from two (2) years to seven (7) years and a fine of not less than
24 Five hundred thousand pesos (P500,000.00) but not more than Two million pesos
25 (P2,000,000.00).

26 (ix) Violation of Section 30 of the Data Privacy Act (Concealment of Security
27 Breaches Involving Sensitive Personal Information) through ICT shall be punished with
28 imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less
29 than Five hundred thousand pesos (P500,000.00) but not more than One million pesos

1 (P1,000,000.00).

2 (x) Violation of Section 33 of the Data Privacy Act (Combination or Series of
3 Acts) through ICT shall be punished with imprisonment ranging from three (3) years to
4 six (6) years and a fine of not less than One million pesos (P1,000,000.00) but not more
5 than Five million pesos (P5,000,000.00).

6 (j) Violation of Section 45 (a) (Hacking) shall be punished with imprisonment ranging
7 from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos
8 (P500,000.00) but not more than Two million pesos (P2,000,000.00).

9 (k) Violation of Section 45 (b) (Cracking) shall be punished with imprisonment ranging
10 from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos
11 (P500,000.00) but not more than Two million pesos (P2,000,000.00).

12 (l) Violation of Section 45 (c) (Phishing) shall be punished with imprisonment ranging
13 from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred
14 thousand pesos (P500,000.00) but not more than One million pesos (P1,000,000.00).

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

17 (i) Violation of Section 25 (a) of the Data Privacy Act (Unauthorized Processing
18 of Personal Information) with hacking, cracking, or phishing shall be punished with
19 imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five
20 hundred thousand pesos (P500,000.00) but not more than Two million pesos
21 (P2,000,000.00).

22 (ii) Violation of Section 25 (b) of the Data Privacy Act (Unauthorized Processing
23 of Sensitive Personal Information) with hacking, cracking, or phishing shall be punished
24 with imprisonment ranging from three (3) years to six (6) years and a fine of not less than
25 Five hundred thousand pesos (P500,000.00) but not more than Four million pesos
26 (P4,000,000.00).

27 (iii) Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal
28 Information Due to Negligence) with hacking, cracking, or phishing shall be punished
29 with imprisonment ranging from one (1) year to three (3) years and a fine of not less than

1 Five hundred thousand pesos (P500,000.00) but not more than Two million pesos
2 (P2,000,000.00).

3 (iv) Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive
4 Personal Information Due to Negligence) with hacking, cracking, or phishing shall be
5 punished with imprisonment ranging from three (3) years to six (6) years and a fine of not
6 less than Five hundred thousand pesos (P500,000.00) but not more than Four million
7 pesos (P4,000,000.00).

8 (v) Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of
9 Personal Information) with hacking, cracking, or phishing shall be punished with
10 imprisonment ranging from six (6) months to two (2) years and a fine of not less than
11 One hundred thousand pesos (P100,000.00) but not more than Five hundred thousand
12 pesos (P500,000.00).

13 (vi) Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of
14 Sensitive Personal Information) with hacking, cracking, or phishing shall be punished
15 with imprisonment ranging from one (1) year to three (3) years and a fine of not less than
16 One hundred thousand pesos (P100,000.00) but not more than One million pesos
17 (P1,000,000.00).

18 (vii) Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal
19 Information for Unauthorized Purposes) with hacking, cracking, or phishing shall be
20 punished with imprisonment ranging from one (1) year and six (6) months to five (5)
21 years and a fine of not less than Five hundred thousand pesos (P500,000.00) but not more
22 than One million pesos (P1,000,000.00).

23 (viii) Violation of Section 28 (b) of the Data Privacy Act (Processing of Sensitive
24 Personal Information for Unauthorized Purposes) with hacking, cracking, or phishing
25 shall be punished with imprisonment ranging from two (2) years to seven (7) years and a
26 fine of not less than Five hundred thousand pesos (P500,000.00) but not more than Two
27 million pesos (P2,000,000.00).

28 (ix) Violation of Section 30 of the Data Privacy Act (Concealment of Security
29 Breaches Involving Sensitive Personal Information) with hacking, cracking, or phishing

1 shall be punished with imprisonment of one (1) year and six (6) months to five (5) years
2 and a fine of not less than Five hundred thousand pesos (P500,000.00) but not more than
3 One million pesos (P1,000,000.00).

4 (x) Violation of Section 33 of the Data Privacy Act (Combination or Series of
5 Acts) with hacking, cracking, or phishing shall be punished with imprisonment ranging
6 from three (3) years to six (6) years and a fine of not less than One million pesos
7 (Php1,000,000.00) but not more than Five million pesos (P5,000,000.00).

8 (n) Violation of Section 46 (a) (Illegal seizure of ICT) shall be punished with
9 imprisonment of *prision correccional* or a fine of not more than Five hundred thousand pesos
10 (P500,000.00), or both.

11 (o) Violation of Section 46 (b) (Aiding and abetting illegal seizure of ICT) shall be
12 punished with imprisonment of *prision correccional* in its minimum period or a fine of not more
13 than Four hundred thousand pesos (P400,000.00), or both.

14 (p) Violation of Section 46 (c) (Arbitrary seizure of ICT) shall be punished with
15 imprisonment of *prision correccional* in its maximum period or a fine of not more than Five
16 hundred thousand pesos (P500,000.00), or both.

17 (q) Violation of Section 46 (d) (Instigating arbitrary seizure of ICT) shall be punished
18 with imprisonment of *prision correccional* or a fine of not more than Five hundred thousand
19 pesos (P500,000.00), or both.

20 (r) Violation of Section 47 (a) (i) (Copyright infringement) – Any person infringing a
21 copyright shall be liable to pay to the copyright proprietor or his assigns or heirs such actual
22 damages, including legal costs and other expenses, as he may have incurred due to the
23 infringement as well as the profits the infringer may have made due to such infringement, and in
24 proving profits the plaintiff shall be required to prove sales only and the defendant shall be
25 required to prove every element of cost which he claims, or, in lieu of actual damages and
26 profits, such damages which to the court shall appear to be just and shall not be regarded as
27 penalty.

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

1 Section.

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

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

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

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

12 (x) Violation of Section 47 (d) (Unreasonable restriction of device privileges) shall be
13 punished with a fine of not less than one hundred thousand pesos (P100,000.00) or more than
14 two million pesos (P2,000,000.00).

15 (y) Violation of Section 48 (Fraud via ICT) shall be punished with imprisonment of
16 *prison correccional* or a fine of at least Two hundred thousand pesos (P200,000.00) up to a
17 maximum amount that is double the amount of damage incurred, whichever is higher, or both
18 imprisonment and fine.

19 (z) Violation of Section 49 (a) (ICT-enabled prostitution) shall be punished with
20 imprisonment of *prison mayor* or a fine of at least Two hundred thousand pesos (P200,000.00)
21 up to a maximum amount of Five hundred thousand pesos (P500,000.00), or both.

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

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

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

1 (iii) Violation of Section 6 of the Anti-Trafficking in Persons Act of 2003 through
2 ICT shall be punished with imprisonment of twenty (20) years and a fine of not less than
3 Two million pesos (P2,000,000.00) but not more than Five million pesos
4 (P5,000,000.00).

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

9 (ab) Violation of Section 50 (a) (ICT-enabled child prostitution) – Violation of Section 5
10 of the Special Protection of Children Against Abuse, Exploitation and Discrimination Act
11 through ICT shall be punished with *reclusion temporal* in its medium period to *reclusion*
12 *perpetua*.

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

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

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

21 (af) Violation of Section 51 (c) (Internet child pornography) – Violation of the Anti-Child
22 Pornography Act through ICT shall be punished according to the provisions of Section 15 of the
23 Anti-Child Pornography Act of 2009 (RA 9775).

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

29 (ah) Violation of Section 51 (e) (Internet expression inimical to the public interest) – This

1 shall only give rise to civil liability and the amount shall be commensurate to the damages
2 caused by the Internet expression.

3 (ai) Violation of Section 52 (b) (Cyberterrorism) – The commission of acts prohibited by
4 the Human Security Act of 2007 through or using devices, equipment, or physical plants
5 connected to the Internet or to telecommunications networks shall be penalized by the applicable
6 provisions of the Human Security Act of 2007.

7 (aj) Violation of Section 52 (c) (ICT-enabled financing of terrorism) – The commission
8 of acts prohibited by the Terrorism Financing Prevention and Suppression Act of 2012 through
9 or using devices, equipment, or physical plants connected to the Internet or to
10 telecommunications networks shall be penalized by the applicable provisions of the Terrorism
11 Financing Prevention and Suppression Act of 2012.

12 (ak) Violation of Section 52 (d) (Cyberespionage) – The commission of acts prohibited
13 by Article 117 of the Penal Code through or using devices, equipment, or physical plants
14 connected to the Internet or to telecommunications networks shall be penalized by the applicable
15 provisions of the Penal Code.

16 SECTION 61. *Penalties for Violations of the Magna Carta for Philippine Internet*
17 *Freedom Affecting Critical Networks and Infrastructure.* – As prescribed by Section 52 (a) of
18 this Act, a penalty one degree higher shall be imposed on the specific violations of the Magna
19 Carta for Philippine Internet Freedom if committed against critical networks or information and
20 communications technology infrastructure.

21 SECTION 62. *Penalties for Other Violations of the Magna Carta for Philippine Internet*
22 *Freedom.* – A fine of not more than Five hundred thousand pesos (P500,000.00) shall be
23 imposed for a violation of other sections of the law not covered by the preceding sections.

24 SECTION 63. *Penalties for Violations of the Magna Carta for Philippine Internet*
25 *Freedom Committed by a Public Official or Employee.* – (a) Except as explicitly provided by the
26 preceding sections, the next higher penalty shall be imposed for a violation or negligence

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

3 (b) If the penalty imposed for the act or negligence resulting in the violation of this Act is
4 civil liability or civil liability and a fine, then an additional penalty of a fine of not less Two
5 hundred thousand pesos (P200,000.00) but not more than Five hundred thousand pesos
6 (P500,000.00) shall be imposed on the public official or employee.

7 SECTION 64. *Liability Under the Data Privacy Act, the Intellectual Property Code, the*
8 *Optical Media Act, the Anti-Child Pornography Act of 2009, the Special Protection of Children*
9 *Against Abuse, Exploitation and Discrimination Act, the Penal Code, and Other Laws.* –(a) A
10 prosecution under this act shall bar any further prosecution of the act as a violation of any
11 provision of the Data Privacy Act, the Intellectual Property Code, the Optical Media Act, the
12 Anti-Child Pornography Act of 2009, the Anti-Trafficking in Persons Act, and other special
13 laws, except:

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

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

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

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

26 (i) if the act was performed through the use of a device, equipment, or physical
27 plant connected to the Internet or to telecommunications networks, or in connivance with
28 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 65. *Competent Law Enforcement Agencies.* – (a) Department of Justice (DOJ). – The Department of Justice shall 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 shall 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 shall 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 66. *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 or she:

(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 67. *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 68. *Extraterritorial Application of the Magna Carta for Philippine Internet Freedom.* – Subject to the provision of existing treaties 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;

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

10 (c) to individual persons who commit any of said crimes within any embassy, consulate,
11 or diplomatic premises belonging to or occupied by the Philippine government in an official
12 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.

19 **Part 9. Implementing Rules and Regulations**

SECTION 69. *Rules and Regulations for the Implementation of the Magna Carta for Philippine Internet Freedom.* – 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 formulate and promulgate the implementing rules and regulations (IRR) of this Act.

1 SECTION 70. *Implementing Rules and Regulations for Information and Communications*
2 *Technology Infrastructure Development.* – The Secretary of Information and Communication
3 Technology, the Secretary of Finance, the Director-General of the National Economic and
4 Development Authority, and the Chairman of the Board of Investments, or their duly authorized
5 and appointed delegates, an appointee from civil society or professional ICT-oriented
6 organizations, and an appointee from the business sector shall formulate and promulgate the
7 implementing rules and regulations (IRR) of this Act towards the development of information
8 and communications technology infrastructure.

9 SECTION 71. *Implementing Rules and Regulations for Cybercrime Law Enforcement.* –
10 The Secretary of Information and Communication Technology, the Secretary of Justice, the
11 Secretary of Interior and Local Government, the Secretary of Social Welfare and Development,
12 the Secretary of Foreign Affairs, the Director-General of the National Bureau of Investigation,
13 and the Director-General of the Philippine National Police, or their duly authorized and
14 appointed delegates, an appointee from the academe, an appointee from civil society, and an
15 appointee from a professional ICT-oriented organization shall formulate and promulgate the
16 implementing rules and regulations (IRR) of this Act towards cybercrime and law enforcement.

17 SECTION 72. *Implementing Rules and Regulations for Information and Communications*
18 *Technology Education, Training, and Human Resources.* –The Secretary of Information and
19 Communication Technology, the Secretary of Education, the Secretary of Science and
20 Technology, the Commissioner of Higher Education, the Director-General of the Technical
21 Education and Skills Development Authority, the Head of the National Telecommunications
22 Training Institute, or their duly authorized and appointed delegates, and an appointee from the
23 academe shall formulate and promulgate the implementing rules and regulations (IRR) of this
24 Act towards information and communications technology education, training and human
25 resources.

26 SECTION 73. *Implementing Rules and Regulations for Information and Communications*

1 *Technology Research and Development.* – The Secretary of Information and Communication
2 Technology, the Secretary of Science and Technology, the Director-General of the National
3 Economic and Development Authority, or their duly authorized and appointed delegates, an
4 appointee from the academe, and an appointee from the business sector, shall formulate and
5 promulgate the rules and regulations (IRR) of this Act towards information and communications
6 technology research and development.

7 SECTION 74. *Implementing Rules and Regulations for National Cyberdefense,*
8 *Cyberintelligence, Counter-Cyberterrorism, and Counter-Cyberespionage.* – (a) The Secretary
9 of National Defense, the Secretary of Interior and Local Government, or their duly authorized
10 and appointed delegates, the Chief of Staff of the Armed Forces of the Philippines (AFP), the
11 commanding general of the unit of the Philippine Air Force tasked with national cyberdefense,
12 the commanding officer of the Intelligence Service, Armed Forces of the Philippines (ISAFP),
13 the commanding officer of the Communication Electronics and Information Systems Service,
14 Armed Forces of the Philippines (CEISSAFP), and the Director-General of the Philippine
15 National Police shall formulate and promulgate the rules and regulations (IRR) of this Act
16 towards ensuring national cyberdefense, cyberintelligence, counter-cyberterrorism, and counter-
17 cyberespionage. The Secretary of Information and Communication Technology shall provide
18 technical advice.

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

(c) 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. *Periodic Review of the Implementing Rules and Regulations of the Magna Carta for Philippine Internet Freedom.* –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.

Part 10. Final Provisions.

SECTION 76. *Appointment of the Secretary 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 77. *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 78. *Preparation of Implementing Rules and Regulations.* – Within ninety (90) days of the release of initial appropriations, implementing rules and regulations shall have been prepared and promulgated.

SECTION 79. *Compliance of Government ICT Infrastructure and Critical Networks, Data, and Internet Infrastructure.* – (a) Within one hundred eighty (180) days from the

1 promulgation of the implementing rules and regulations, government agencies and
2 instrumentalities shall have secured their private network and data infrastructure. Penalties as
3 prescribed by this Act shall be imposed for noncompliance.

4 (b) Within two hundred seventy days (270) days from the promulgation of the
5 implementing rules and regulations, government agencies and instrumentalities shall have
6 secured their public network, data, and Internet infrastructure. Penalties as prescribed by this Act
7 shall be imposed for noncompliance.

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

14 (d) Within ninety (90) days from the promulgation of the implementing rules and
15 regulations, all Internet service providers, Internet exchanges, Internet data centers, Internet
16 gateway facilities, telecommunications entities, and persons providing Internet connection,
17 network, or data transmission services shall have met the minimum standards of
18 interconnectivity and interoperability of their information and communications technology
19 infrastructure. Administrative penalties shall be prescribed for noncompliance.

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

25 SECTION 80. *Public Information Campaign for the Magna Carta for Philippine Internet*
26 *Freedom and its Implementing Rules and Regulations.* – (a) The Office of the President, the
27 Presidential Communications Development and Strategic Planning Office or its successor
28 agency, the Philippine Information Agency or its successor agency, and the Department of

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

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

9 SECTION 81. *Initial Funding Requirements.* – (a) DICT – An initial appropriation of
10 fifteen million pesos (P15,000,000) shall be drawn from the national government for purposes of
11 the establishment and operation of the DICT, exclusive of the existing appropriations of its
12 subordinate agencies, which shall accrue to the DICT budget.

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

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

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

19 (e) IRR – An initial appropriation of five million pesos (P5,000,000), to be disbursed by
20 the Secretary of Information and Communications Technology, shall be drawn from the national
21 government for purposes of the preparation of the Implementing Rules and Regulations of this
22 Act.

23 (f) PIA – An appropriation of five million pesos (P5,000,000) shall be drawn from the
24 national government for purposes of the information dissemination campaign on this Act by the
25 PIA.

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

1 SECTION 82. *Succeeding Appropriations.* – Such sums as may be necessary for the
2 implementation of this Act shall be included in the agencies' yearly budgets under the General
3 Appropriations Act.

4 SECTION 83. *Separability Clause.* – If any provision or part hereof is held invalid or
5 unconstitutional, the remainder of the law or the provisions not otherwise affected shall remain
6 valid and subsisting.

7 SECTION 84. *Repealing Clause.* – Any law, presidential decree or issuance, executive
8 order, letter of instruction, administrative order, rule, or regulation contrary to, or inconsistent
9 with, the provisions of this Act is hereby repealed, modified, or amended accordingly.

10 SECTION 85. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its
11 publication in at least (2) newspapers of general circulation.