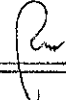


FIFTEENTH CONGRESS OF THE REPUBLIC)
OF THE PHILIPPINES)
First Regular Session)



'11 MAY -3 P 6:44

SENATE

RECEIVED BY: 

COMMITTEE REPORT NO. **30**

Submitted jointly by the Committees on Science and Technology; Constitutional Amendments, Revision of Codes and Laws; Education, Arts and Culture; Justice and Human Rights; Trade and Commerce; Public Information and Mass Media and Finance on **MAY - 3 2011**.

Re: Senate Bill No. **2796**

Recommending its approval in substitution of Senate Bill Nos. 14, 52, 134, 275, 665, 828, 983, 1081, 1475, 1963, 2214, 2451, 2534, 2674, 2721, taking into consideration Senate Resolution Nos. 75, 164 and 254.

Sponsor: Senator Edgardo J. Angara

MR. PRESIDENT:

The Committees on Science and Technology; Constitutional Amendments, Revision of Codes and Laws; Education, Arts and Culture; Justice and Human Rights; Trade and Commerce; Public Information and Mass Media and Finance to which were referred Senate Bill No. 14, introduced by Senator Trillanes, entitled:

**“AN ACT
DEFINING CYBERCRIME, PROVIDING FOR PREVENTION, SUPPRESSION AND
IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES”**

S. No. 52, introduced by Senator Angara, entitled:

**“AN ACT
DEFINING CYBERCRIME, PROVIDING FOR PREVENTION, INVESTIGATION AND
IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES”**

S. No. 134, introduced by Senator Enrile, entitled:

**“AN ACT
DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, SUPPRESSION
AND IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES”**

S. No. 275, introduced by Senator Trillanes, entitled:

**“AN ACT
PROTECTING CONSUMERS BY PROHIBITING THE UNAUTHORIZED AND
DECEPTIVE INSTALLATION OF SPYWARE IN COMPUTERS, PROVIDING
PENALTIES THEREFOR, AND FOR OTHER PURPOSES”**

S. No. 665, introduced by Senator Estrada, entitled

**“AN
ACT TO PREVENT FRAUDULENT ACQUISITION OF A PHILIPPINE DOMAIN OR
.PH DOMAIN NAME OVER THE INTERNET AND FOR OTHER PURPOSES”**

S.No. 828, introduced by Senator Estrada, entitled:

**“AN
ACT TO PROMOTE AND GOVERN THE DEVELOPMENT OF VOICE OVER
INTERNET PROTOCOL IN THE PHILIPPINES”**

S. No. 983, introduced by Senator Lapid, entitled:

**“AN ACT
PROVIDING PROTECTION AGAINST COMPUTER FRAUD AND ABUSES AND
OTHER CYBER-RELATED FRAUDULENT ACTIVITIES, PROVIDING PENALTIES
THEREFOR, AND FOR OTHER PURPOSES”**

S. No. 1081, introduced by Senator Villar, entitled:

**“AN ACT
PREVENTING AND PENALIZING COMPUTER FRAUD ABUSES AND OTHER
CYBER-RELATED FRAUDULENT ACTIVITIES AND CREATING FOR THE
PURPOSE THE CYBER CRIME INVESTIGATION AND COORDINATING CENTER
PRESCRIBING ITS POWERS AND FUNCTIONS, AND APPROPRIATING FUNDS
THEREFOR”**

S. No. 1475, introduced by Senator Defensor Santiago, entitled:

**“AN ACT
PROTECTING CONSUMERS FROM COMPUTER GRAYWARE”**

S. No. 1963, introduced by Senator Defensor Santiago, entitled:

**“AN ACT
TO REGULATE THE UNAUTHORIZED INSTALLATION OF COMPUTER
SOFTWARE AND TO REQUIRE THE CLEAR DISCLOSURE TO COMPUTER USERS
OF CERTAIN COMPUTER SOFTWARE FEATURES THAT MAY POSE A THREAT
TO USER PRIVACY”**

S. No. 2214, introduced by Senator Defensor Santiago, entitled:

**“AN ACT
TO CRIMINALIZE INTERNET SCAMS INVOLVING FRAUDULENTLY OBTAINING
PERSONAL INFORMATION”**

S. No. 2451, introduced by Senator Villar, entitled:

**“DEFINING THE CRIME OF INTERNET AND TELECOMMUNICATIONS
PHISHING, PROVIDING PENALTIES THEREFOR AND FOR OTHER PURPOSES”**

S. No. 2534, introduced by Senator Marcos, entitled:

**“AN ACT
DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION,
INVESTIGATION AND IMPOSITION OF PENALTIES THEREFOR AND FOR
OTHER PURPOSES”**

S. No. 2674, introduced by Senator Defensor Santiago, entitled:

**“AN
ACT AUTHORIZING THE COMMISSION ON HIGHER EDUCATION TO
ESTABLISH A PROGRAM TO AWARD GRANTS TO INSTITUTIONS OF HIGHER
EDUCATION FOR THE ESTABLISHMENT OR EXPANSION OF CYBERSECURITY
PROFESSIONAL DEVELOPMENT PROGRAMS”**

S. No. 2721, introduced by Senator Revilla, entitled:

**“AN ACT
DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION
AND IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES”**

S. Resolution No. 75, introduced by Senator Defensor Santiago, entitled:

**“RESOLUTION DIRECTING THE PROPER SENATE COMMITTEE TO CONDUCT
AN INQUIRY, IN AID OF LEGISLATION, ON THE REPORTED SOCIAL
NETWORKING DANGERS WITH A VIEW TO ENJOIN THE PUBLIC TO
UNDERTAKE SUFFICIENT PRECAUTIONARY MEASURES AGAINST ALLEGED
ILLICIT ACTIVITIES OF SO-CALLED CYBERCRIMINAL”**

S. Resolution No. 164, introduced by Senator Villar, entitled:

**“RESOLUTION URGING THE COMMITTEES ON SCIENCE AND TECHNOLOGY;
AND PUBLIC INFORMATION AND MASS MEDIA TO CONDUCT AN INQUIRY, IN
AID OF LEGISLATION, ON THE INCREASING OCCURRENCE OF CYBER
STALKING CASES AND THE MODUS OPERANDI ADOPTED IN THE INTERNET
TO PERPETUATE CRIMES WITH THE END IN VIEW OF FORMULATING
LEGISLATION AND POLICY MEASURES GEARED TOWARDS CURBING
STALKING AND OTHER CYBER CRIMES AND PROTECT ONLINE USERS IN THE
COUNTRY” and**

S. Resolution No. 254, introduced by Senator Villar, entitled:

**“RESOLUTION URGING THE COMMITTEES ON SCIENCE AND TECHNOLOGY;
AND PUBLIC INFORMATION AND MASS MEDIA AND OTHER APPROPRIATE
COMMITTEES TO CONDUCT AN INQUIRY, IN AID OF LEGISLATION, ON THE
INCREASING INCIDENCE OF HARASSMENT ON THE INTERNET OR CYBER-
BULLYING VIS-À-VIS PRESENT STATUTES AND LEGISLATION WITH THE END
IN VIEW OF PROTECTING INTERNET USERS”**


have considered the same and have the honor to report them back to the Senate with the recommendation that the attached Senate Bill No. 2796, prepared by the Committees, entitled:


**“AN ACT
DEFINING CYBERCRIME, PROVIDING FOR PREVENTION, INVESTIGATION AND
IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES”**


be approved in substitution of Senate Bill Nos. 14, 52, 134, 275, 665, 828, 983, 1081, 1475, 1963, 2214, 2451, 2534, 2674 and 2721, taking into consideration Senate Resolution Nos. 75, 164 and 254, with Senators Trillanes, Angara, Enrile, Estrada, Lapid, Villar, Defensor Santiago, Marcos and Revilla as authors thereof.


Respectfully submitted:

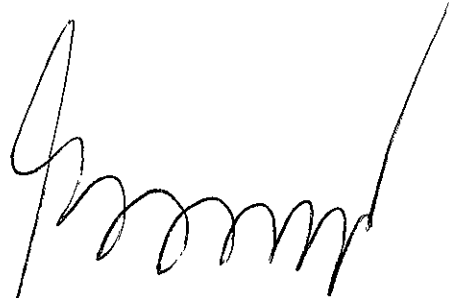
Chair:

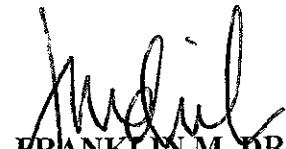

SEN. MIRIAM DEFENSOR SANTIAGO
Chairman
Committee on Constitutional Amendments
Member, Committees on Science & Technology;
Trade & Commerce; Finance


SEN. EDGARDO J. ANGARA
Chairman
Committees on Science and Technology;
Education, Arts & Culture & Subcom B
Finance
Vice-Chair, Committee on Constitutional
Amendments, Revision of Codes and Laws
Member, Committee on Trade & Commerce

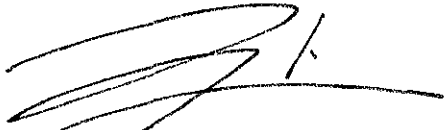

SEN. FRANCIS "Chiz" G. ESCUDERO
Chairman
Committee on Justice and Human Rights
Member, Committee on Finance


SEN. MANNY VILLAR
Chairman
Trade and Commerce
Vice-Chairman, Committee on Public
Information & Mass Media
Member, Committees on Constitutional
Amendments, Revision of Codes and Laws,
Science & Technology; Justice & Human
Rights; Education, Arts & Culture; Finance


SEN. GREGORIO B. HONASAN II
Chairman
Public Information and Mass Media
Member, Committee on Finance


SEN. FRANKLIN M. DRILON
Chairman, Subcom A, Finance
Member, Committees on Education, Arts &
Culture; Constitutional Amendments,
Revision of Codes and Laws; Justice on
Human Rights; Education, Arts & Culture;
Public Information & Mass Media

Vice-Chair:



SEN. JUAN MIGUEL F. ZUBIRI
Vice-Chairman
Committee on Science and Technology
Member, Committees on Education, Arts
& Culture; Trade & Commerce; Finance;
Science & Technology; Constitutional Amendments,
Revision of Codes & Laws

will amend


SEN. TEOFISTO L. GUINGONA III
Vice-Chairman
Committee on Justice & Human Rights
Member, Committees on Education, Arts &
Culture; Finance

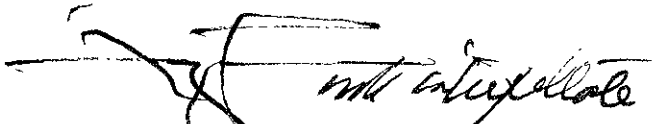


SEN. LOREN B. LEGARDA
Vice-Chairman
Committees on Education, Arts & Culture;
Public Information & Mass Media
Member, Committees on Finance, Subcom B; Science & Technology;
Trade & Commerce; Justice & Human Rights

Members:




SEN. FERDINAND R. MARCOS, JR.
Committees on Science & Technology;
Trade & Commerce; Public Information
& Mass Media; Finance




SEN. FRANCIS N. PANGILINAN
Committees on Science & Technology
and Finance

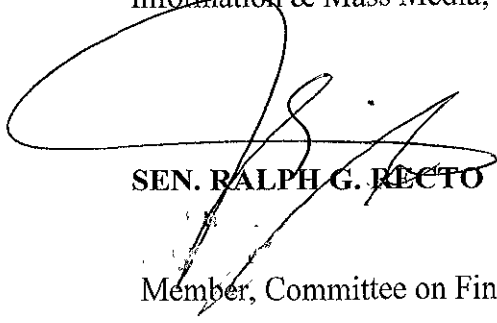
SEN. PANFILO M. LACSON
Committee on Constitutional Amendments,
Revision of Codes & Laws



SEN. MANUEL "Lito" M. LAPID
Committees on Constitutional Amendments,
Revision of Codes & Laws; Public
Information & Mass Media; Finance



SEN. PIA CAYETANO
Member, Committees on Education,
Arts & Culture; Trade & Commerce &
Public Information and Mass Media



SEN. RALPH G. RECTO
Member, Committee on Finance

SEN. ANTONIO "Sonny" F. TRILLANES IV
Committees on Education, Arts & Culture &
Justice & Human Rights

SEN. RAMON BONG REVILLA, JR.
Committees on Education, Arts & Culture;
Justice & Human Rights; Trade &
Commerce; Public Information & Mass
Media

SEN. SERGIO R. OSMEÑA III
Committees on Education, Arts & Culture;
Justice & Human Rights; Public Information &
Mass Media; Finance

SEN. JOKER P. ARROYO
Committees on Education, Arts & Culture;
Justice & Human Rights; Trade &
Commerce; Finance

Ex-Officio Members:

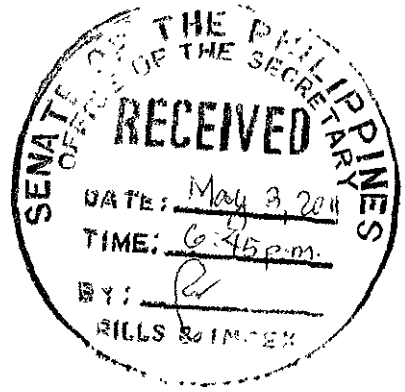
SEN. JINGGOY EJERCITO ESTRADA
President Pro-Tempore

SEN. VICENTE C. SOTTO III
Majority Leader

SEN. ALAN PETER "Compañero" S. CAYETANO
Minority Leader

HON. JUAN PONCE ENRILE
Senate President
Pasay City

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



SENATE
S. No. **2796**

Prepared jointly by the Committees on Science and Technology; Constitutional Amendments, Revision of Codes and Laws; Education, Arts and Culture; Justice and Human Rights; Trade and Commerce; Public Information and Mass Media and Finance with Senators Trillanes, Angara, Enrile, Estrada, Lapid, Villar, Defensor Santiago, Marcos and Revilla as authors

**AN ACT DEFINING CYBERCRIME,
PROVIDING FOR PREVENTION, INVESTIGATION AND IMPOSITION OF
PENALTIES THEREFOR AND FOR OTHER PURPOSES**

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

CHAPTER I – PRELIMINARY PROVISIONS

SECTION 1. Title. -- This Act shall be known as the “Cybercrime Prevention Act of 2011”.

SEC. 2. Declaration of Policy. -- The State recognizes the vital role of information and communications industries such as content production, telecommunications, broadcasting, electronic commerce, and data processing, in the nation’s overall social and economic development. The State also recognizes the importance of providing an environment conducive to the development, acceleration, and rational application and exploitation of information and communications technology to attain free, easy, and intelligible access to exchange and/or delivery of information; and the need to protect and safeguard the integrity of computer, computer and communications systems, networks, and databases, and the confidentiality, integrity, and availability of information and data stored therein, from all forms of misuse, abuse, and illegal access by making punishable under the law such conduct or conducts. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36

SEC. 3. *Definition of Terms.* -- For purposes of this Act, the following terms are hereby defined as follows:

- a) Access -- refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network;
- b) Alteration - refers to the modification or change, in form or substance, of an existing computer data or program;
- c) Communication - refers to the transmission of information including voice and non-voice data;
- d) Computer system - means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data. It covers any type of computer device including devices with data processing capabilities like mobile phones and also computer networks. The device consisting of hardware and software may include input, output and storage facilities which may stand alone or be connected in a network or other similar devices. It also includes computer-data storage devices or medium.
- e) Computer Data - refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system including a program suitable to cause a computer system to perform a function and includes electronic documents and/or electronic data messages;
- f) Computer Program -- refers to a set of instructions executed by the computer;
- g) Without Right -- refers to either: (1) conduct undertaken without or in excess of authority; or (ii) conduct not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law;
- h) Database -- refers to a representation of information, knowledge, facts, concepts, or instructions which are being prepared, processed or stored or

1 have been prepared, processed or stored in a formalized manner and which are
2 intended for use in a computer system;

3
4 i) Interception – refers to listening to, recording, monitoring or surveillance of
5 the content of communications, including procuring of the content of data,
6 either directly, through access and use of a computer system or indirectly,
7 through the use of electronic eavesdropping or tapping devices, at the same
8 time that the communication is occurring;

9
10 j) Service Provider – refers to :

11
12 i. any public or private entity that provides to users of its service the
13 ability to communicate by means of a computer system, and

14
15 ii. any other entity that processes or stores computer data on behalf of
16 such communication service or users of such service;

17
18 k) Subscriber's Information – refers to any information contained in the form of
19 computer data or any other form that is held by a service provider, relating to
20 subscribers of its services other than traffic or content data and by which can
21 be established;

22
23 i. The type of communication service used, the technical provisions
24 taken thereto and the period of service;

25
26 ii. The subscriber's identity, postal or geographic address, telephone and
27 other access numbers, any assigned network address, billing and
28 payment information, available on the basis of the service agreement
29 or arrangement;

30
31 iii. Any other available information on the site of the installation of
32 communication equipment, available on the basis of the service
33 agreement or arrangement.

34
35 l) Traffic Data or Non-Content Data – refers to any computer data other than the
36 content of the communication, including but not limited to the

1 communication's origin, destination, route, time, date, size, duration, or type
2 of underlying service.

3
4
5
6 **CHAPTER II – PUNISHABLE ACTS**
7

8 **SEC. 4. *Cybercrime Offenses.*** -- The following acts constitute the offense of
9 cybercrime punishable under this Act:

10
11 A. Offenses against the confidentiality, integrity and availability of computer data
12 and systems:

13
14 1. Illegal Access - The intentional access to the whole or any part of a computer
15 system without right.

16
17 2. Illegal Interception - The intentional interception made by technical means
18 without right of any non-public transmission of computer data to, from, or
19 within a computer system including electromagnetic emissions from a
20 computer system carrying such computer data: Provided, however, That it
21 shall not be unlawful for an officer, employee, or agent of a service provider,
22 whose facilities are used in the transmission of communications, to intercept,
23 disclose, or use that communication in the normal course of his employment
24 while engaged in any activity that is necessary to the rendition of his service
25 or to the protection of the rights or property of the service provider, except
26 that the latter shall not utilize service observing or random monitoring except
27 for mechanical or service control quality checks;

28
29 3. Data interference - the intentional or reckless alteration of computer data
30 without right.

31
32 4. System Interference - the intentional or reckless hindering without right of the
33 functioning of a computer system by inputting, transmitting, deleting or
34 altering computer data or program.

35
36 5. Misuse of Devices –
37

1 a. The use, production, sale, procurement, importation, distribution, or
2 otherwise making available, without right, of:

3
4 i. a device, including a computer program, designed or adapted primarily
5 for the purpose of committing any of the offenses under this Act; or
6

7 ii. a computer password, access code, or similar data by which the whole
8 or any part of a computer system is capable of being accessed with
9 intent that it be used for the purpose of committing any of the offenses
10 under this Act;.

11
12 b. The possession of an item referred to in paragraphs 5(a)(i) or (ii) above
13 with intent to use said devices for the purpose of committing any of the
14 offenses under this Section.
15

16 Provided, That no criminal liability shall attach when the use, production, sale,
17 procurement, importation, distribution, or otherwise making available, or
18 possession of computer devices/data referred to is for the authorized testing of a
19 computer system.
20

21 B. Computer-related Offenses:
22

23 1. Computer-related Forgery – (a) the intentional input, alteration, or deletion of
24 any computer data without right resulting in inauthentic data with the intent
25 that it be considered or acted upon for legal purposes as if it were authentic,
26 regardless whether or not the data is directly readable and intelligible; (b) the
27 act of knowingly using computer data which is the product of computer-
28 related forgery as defined herein, for the purpose of perpetuating a fraudulent
29 or dishonest design.
30

31 2. Computer-related Fraud -- the intentional and unauthorized input, alteration, or
32 deletion of computer data or program or interference in the functioning of a
33 computer system, causing damage thereby, with the intent of procuring an
34 economic benefit for oneself or for another person or for the perpetuation of a
35 fraudulent or dishonest activity; Provided, that if no damage has yet been
36 caused, the penalty imposable shall be one degree lower.
37

1 C. Content-related Offenses:

- 2
- 3 1. Cybersex – any person who establishes, maintains or controls, directly or
4 indirectly, any operation for sexual activity or arousal with the aid of or
5 through the use of a computer system, for a favor or consideration.
6
 - 7 2. Child Pornography - refers to any representation, whether visual, audio, or
8 written combination thereof, by electronic, mechanical, digital, optical,
9 magnetic or any other means, of child engaged or involved in real or
10 simulated explicit sexual activities.
11

12 For the purpose of this Act, a "child" refers to a person below eighteen (18) years of age
13 or over, but is unable to fully take care of himself/herself from abuse, neglect, cruelty,
14 exploitation or discrimination because of a physical or mental disability or condition. A
15 child shall also refer to: (a) a person regardless of age who is presented, depicted or
16 portrayed as a child as defined herein; and (b) computer-generated, digitally or manually
17 crafted images or graphics of a person who is represented or who is made to appear to be
18 a child as defined herein.
19

20 The unlawful or prohibited acts constituting child pornography shall be defined
21 and punishable by Republic Act No. 9775 or the Anti-Child Pornography Law.
22

- 23 3. Unsolicited Commercial Communications. -- The transmission of commercial
24 electronic communication with the use of computer system which seek to
25 advertise, sell, or offer for sale products and services are prohibited unless:
26
 - 27 a. There is a prior affirmative consent from the recipient; or
 - 28 b. The following conditions are present:
 - 29 i. The commercial electronic communication contains a simple,
30 valid, and reliable way for the recipient to reject receipt of further
31 commercial electronic messages ('opt-out') from the same source;
 - 32 ii. The commercial electronic communication does not purposely
33 disguise the source of the electronic message; and
 - 34 iii. The commercial electronic communication does not purposely
35 include misleading information in any part of the message in order
36 to induce the recipients to read the message.
37

1 Any person found guilty of any of the punishable acts enumerated in Section 5
2 shall be punished with imprisonment one degree lower than that of the prescribed penalty
3 for the offense or a fine of at least One Hundred Thousand Pesos (PhP100,000.00) but
4 not exceeding Five Hundred Thousand Pesos (PhP500,000.00) or both.

5
6 **SEC. 8. Corporate Liability.** -- When any of the punishable acts herein defined
7 are knowingly committed on behalf of or for the benefit of a juridical person, by a natural
8 person acting either individually or as part of an organ of the juridical person, who has a
9 leading position within in, based on (a) a power of representation of the juridical person,
10 (b) an authority to take decisions on behalf of the juridical person, or (c) an authority to
11 exercise control within the juridical person, the juridical person shall be held liable for a
12 fine equivalent to at least double the fines imposable in Section 7 up to a maximum of
13 Ten Million Pesos (Php10,000,000.00).

14
15 If the commission of any of the punishable acts herein defined was made possible
16 due to the lack of supervision or control by a natural person referred to and described in
17 the preceding paragraph, for the benefit of that juridical person by a natural person acting
18 under its authority, the juridical person shall be held liable for a fine equivalent to at least
19 double the fines imposable in Section 7 up to a maximum of Five Million Pesos
20 (Php5,000,000.00).

21
22 The liability imposed on the juridical person shall be without prejudice to the
23 criminal liability of the natural person who has committed the offence.

24 25 26 **CHAPTER IV – ENFORCEMENT AND IMPLEMENTATION**

27
28 **SEC. 9. Real-time Collection of Computer Data.** -- Law enforcement authorities,
29 with due cause, and upon securing a court warrant, shall be authorized to collect or record
30 by technical or electronic means, and service providers are required to collect or record
31 by technical or electronic means, and/or to cooperate and assist law enforcement
32 authorities in the collection or recording of, traffic data, in real-time, associated with
33 specified communications transmitted by means of a computer system.

34
35 **SEC. 10. Preservation of Computer Data.** -- The integrity of traffic data and
36 subscriber information relating to communication services provided by a service provider
37 shall be preserved for a minimum period of six (6) months from the date of the

1 transaction. Content data shall be similarly preserved for six (6) months from the data of
2 receipt of the order from law enforcement authorities requiring its preservation.

3
4 Law enforcement authorities may order a one-time extension for another six (6)
5 months provided that once computer data preserved, transmitted or stored by a service
6 provider is used as evidence in a case, the mere furnishing to such service provider of the
7 transmittal document to the Office of the Prosecutor shall be deemed a notification to
8 preserve the computer data until the termination of the case.

9
10 The service provider ordered to preserve computer data shall keep confidential the
11 order and its compliance.

12
13 **SEC. 11. *Disclosure of Computer Data.*** -- Law enforcement authorities, upon
14 securing a court warrant, shall issue an order requiring any person or service provider to
15 disclose or submit subscriber's information, traffic data or relevant data in his/its
16 possession or control within seventy two (72) hours from receipt of the order in relation
17 to a valid complaint officially docketed and assigned for investigation and the disclosure
18 is necessary and relevant for the purpose of investigation.

19
20 **SEC. 12. *Search, Seizure, and Examination of Computer Data.*** -- Where a
21 search and seizure warrant is properly issued, the law enforcement authorities shall
22 likewise have the following powers and duties:

23
24 Within the time period specified in the warrant, to conduct interception, as
25 defined in this Act, content of communications, procure the content of data either
26 directly, through access and use of computer system, or indirectly, through the use of
27 electronic eavesdropping or tapping devices, in real time or at the same time that the
28 communication is occurring and:

- 29
30 a. To secure a computer system or a computer data storage medium;
31 b. To make and retain a copy of those computer data secured;
32 c. To maintain the integrity of the relevant stored computer data;
33 d. To conduct examination of the computer data storage medium; and
34 e. To render inaccessible or remove those computer data in the accessed
35 computer or computer and communications network.

36

1 Pursuant thereof, the law enforcement authorities may order any person who has
2 knowledge about the functioning of the computer system and the measures to protect and
3 preserve the computer data therein to provide, as is reasonable, the necessary
4 information, to enable the undertaking of the search, seizure and examination.

5
6 Law enforcement authorities may request for an extension of time to complete the
7 examination of the computer data storage medium and to make a return thereon but in no
8 case for a period longer than thirty (30) days from date of approval by the court.

9
10 **SEC. 13. *Non-compliance.*** -- Failure to comply with the provisions of Chapter
11 IV hereof specifically the orders from law enforcement authorities shall be punished as a
12 violation of P.D. No. 1829 with imprisonment of *prision correctional* in its maximum
13 period or a fine of One Hundred Thousand Pesos (Php100,000.00) or both, for each and
14 every non-compliance with an order issued by law enforcement authorities.

15
16 **SEC. 14. *Duties of Law Enforcement Authorities.*** -- To ensure that the technical
17 nature of cybercrime and its prevention is given focus and considering the procedures
18 involved for international cooperation, law enforcement authorities specifically the
19 computer or technology crime divisions or units responsible for the investigation of
20 cybercrimes are required to submit timely and regular reports including pre-operation,
21 post-operation and investigation results and such other documents as may be required to
22 the Department of Justice (DOJ) for review and monitoring.

23
24
25 **CHAPTER V – JURISDICTION**

26
27 **SEC.15. *Jurisdiction.*** -- The Regional Trial Court shall have jurisdiction over
28 any violation of the provisions of this Act including any violation committed by a
29 Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the
30 elements was committed within the Philippines or committed with the use of any
31 computer system wholly or partly situated in the country, or when by such commission
32 any damage is caused to a natural or juridical person who, at the time the offense was
33 committed, was in the Philippines.

1 **CHAPTER VI – INTERNATIONAL COOPERATION**
2

3 **SEC. 16. *General principles relating to international cooperation.*** -- All
4 relevant international instruments on international cooperation in criminal matters,
5 arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws,
6 to the widest extent possible for the purposes of investigations or proceedings concerning
7 criminal offenses related to computer systems and data, or for the collection of evidence
8 in electronic form of a criminal offense shall be given full force and effect.
9

10 **SEC. 17. *Applicability of the Convention on Cybercrime.*** -- The provisions of
11 Chapter III of the Convention on Cybercrime shall be directly applicable in the
12 implementation of this Act as it relates to international cooperation taking into account
13 the procedural laws obtaining in the jurisdiction.
14
15

16 **CHAPTER VII – COMPETENT AUTHORITIES**
17

18 **SEC. 18. *Department of Justice.*** – The Department of Justice (DOJ) shall be
19 responsible for extending immediate assistance for the purpose of investigations or
20 proceedings concerning criminal offenses related to computer systems and data, or for the
21 collection of electronic evidence of a criminal offense and to otherwise ensure that the
22 provisions of this law are complied. In this regard, there is hereby created a DOJ Office
23 of Cybercrime for facilitating or directly carrying out the provisions of technical advice,
24 preservation of data, collection of evidence, giving legal information and locating
25 suspects and all other cybercrime matters related to investigation and reporting issues.
26

27 **SEC. 19. *Commission on Information and Communications Technology.*** – The
28 Commission on Information and Communications Technology (CICT) shall be
29 responsible for formulating and implementing a national cyber security plan and
30 extending immediate assistance for the suppression of real-time commission of
31 cybercrime offenses through a computer emergency response team (CERT). In this
32 regard, there is hereby created a CICT National Cyber Security Office to carry out the
33 above responsibilities and all other matters related to cybercrime prevention and
34 suppression, including capacity building.
35
36
37

1 **CHAPTER VIII – CYBERCRIME INVESTIGATION AND**
 2 **COORDINATION CENTER**

3
 4 **SEC. 20. *Cybercrime Investigation and Coordinating Center.*** -- There is hereby
 5 created, within thirty (30) days from the effectivity of this Act, a Cybercrime
 6 Investigation and Coordinating Center, hereinafter referred to as CICC, under the control
 7 and supervision of the Office of the President, to formulate and implement the national
 8 cyber security plan.

9
 10 **SEC. 21. *Composition.*** -- The CICC shall be headed by the Chairman of the
 11 Commission on Information and Communications Technology as Chairman; with the
 12 Director of the NBI as Vice-Chairman; Chief of the PNP; Chief of the National
 13 Prosecution Service (NPS); and the Head of the National Computer Center (NCC) as
 14 members.

15
 16 The CICC shall be manned by a secretariat of selected personnel and
 17 representatives from the different participating agencies.

18
 19 **SEC. 22. *Powers and Functions.*** -- The CICC shall have the following powers
 20 and functions:

- 21 a. To prepare and implement appropriate and effective measures to prevent and
 22 suppress cybercrime activities as provided in this Act;
 23 b. To monitor cybercrime cases being handled by participating law enforcement
 24 and prosecution agencies;
 25 c. To facilitate international cooperation on intelligence, investigations, training
 26 and capacity building related to cybercrime prevention, suppression and
 27 prosecution;
 28 d. To coordinate the support and participation of the business sector, local
 29 government units, and non-government organizations in cybercrime
 30 prevention programs and other related projects;
 31 e. To recommend the enactment of appropriate laws, issuances, measures and
 32 policies;
 33 f. To call upon any government agency to render assistance in the
 34 accomplishment of the CICC's mandated tasks and functions;
 35 g. To perform such other functions and duties necessary for the proper
 36 implementation of this Act.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CHAPTER IX – FINAL PROVISIONS

SEC. 23. Appropriations. -- The amount of ten million pesos (Php10,000,000.00) shall be appropriated annually for the implementation of this Act.

SEC. 24. Implementing Rules and Regulations. - The Department of Justice in consultation with the Commission on Information and Communication Technology shall formulate the necessary rules and regulations for the effective implementation of this Act including the creation and establishment of a national cyber security office with the relevant computer emergency response council or team.

SEC. 25. Separability Clause. -- If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

SEC. 26. Repealing Clause. --. All laws, decrees, or rules inconsistent with this Act are hereby repealed or modified accordingly. Section 33 of Republic Act No. 8792 or the Electronic Commerce Act is hereby modified accordingly.

SEC. 27. Effectivity. -- This Act shall take effect fifteen (15) days after the completion of its publication in the Official Gazette or in at least two (2) newspapers of general circulation.

Approved.

