CONGRESS OF THE PHILIPPINES FOURTEENTH CONGRESS Third Regular Session

HOUSE OF REPRESENTATIVES

H. No. 6794

BY REPRESENTATIVES SINGSON (E.), ANGARA, DEL MAR, NICOLAS, TEODORO, ALMARIO, SANTIAGO (J.), JOSON, LAZATIN, CODILLA, UNGAB, ABLAN, VILLAR, SANTIAGO (N.), FUA, CHATTO, LIM, CUA (J.), VILLAROSA, NOGRALES, GONZALES (N.) AND DE GUZMAN, PER COMMITTEE REPORT NO. 2342

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

Be it enacted by the Senate and 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 2009".
SEC. 2. Declaration of Policy The State recognizes the increasingly
vital role of information and communications technology (ICT) as an enabler
of key industries such as, banking, broadcasting, business process outsourcing,
electronic commerce and telecommunications, and as a driving force for the
nation's overall social and economic development. The State also recognizes
the importance of providing an environment conducive to the development,

1 acceleration and application of ICT to attain free, easy and intelligible access to exchange and/or delivery of information; and the need to protect and 2 3 safeguard the integrity of computer and communications systems, networks and database, and the confidentiality, integrity and availability of information and 4 5 data stored therein, from all forms of misuse, abuse and illegal access by 6 making such conduct punishable under the law. In this light, the State shall 7 adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation and prosecution at both the domestic 8 9 and international levels, and by providing arrangements for fast and reliable 10 international cooperation.

11 12

· • `

* `

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, storage of
data in, retrieval of data from, or otherwise making use of any resource of a
computer system.

(b) Alteration refers to the modification or change, in form orsubstance, of an existing computer data or program.

18 (c) Communication refers to the transmission of information, including
19 voice and non-voice data.

20 (d) Computer system refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs 21 automated processing of data. It covers any type of device with data 22 23 processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, 24 output and storage components which may stand alone or be connected in a 25 network or other similar devices. It also includes computer data storage 26 27 devices or media.

(e) Computer data refers to any representation of facts, information or 1 2 concepts in a form suitable for processing in a computer system, including any 3 program capable of causing a computer system to perform a function, as well 4 as electronic documents or electronic data messages.

5

, ``

r `

(f) Computer program refers to a set of instructions executed by the 6 computer to achieve intended results.

7 (g) Conduct without right refers to either: (1) conduct undertaken 8 without or in excess of authority; or (2) conduct not covered by established 9 legal defenses, excuses, court orders, justifications or relevant principles under 10 the law.

11 (h) Database refers to a representation of information, knowledge, facts, concepts or instructions which are being prepared, processed or stored or 12 13 have been prepared, processed or stored in an organized manner and which are 14 intended for use in a computer system.

15 (i) Interception refers to listening to, recording, monitoring or surveillance of the content of communications, including procurement of the 16 17 content of data, either directly, through access and use of a computer system or 18 indirectly, through the use of electronic eavesdropping or tapping devices, at 19 the same time that the communication is occurring.

20 (i) *Phishing* refers to the act of securing personal information such as 21 username, password, bank account numbers and credit card details for the 22 purpose of using it in fraud, or for participating in fraudulent business 23 practices, or for the purpose of identity theft and misrepresentation.

(k) Service provider refers to: (1) any public or private entity that 24 provides to users of its service the ability to communicate by means of a 25 computer system; or (2) any other entity that processes or stores computer data 26 27 on behalf of such communication service or users of such service.

3

1 (1) Subscriber's information refers to any information contained in the 2 form of computer data or any other form that is held by a service provider, 3 relating to subscribers of its services other than traffic or content data and by 4 which can be established: (1) the type of communication service used, the 5 technical provisions taken thereto and the period of service; (2) the 6 subscriber's identity, postal or geographic address, telephone and other access 7 number, any assigned network address, billing and payment information. 8 available on the basis of the service agreement or arrangement; or (3) any other 9 available information on the site of the installation of communication 10 equipment, available on the basis of the service agreement or arrangement.

11 (m) *Traffic data or non-content data* refers to any computer data other 12 than the content of the communication including, but not limited to, the 13 communication's origin, destination, route, time, date, size, duration or type of 14 underlying service.

CHAPTER II

PUNISHABLE ACTS

15

· ` `

۰ ،

16

17 SEC. 4. *Cybercrime Offenses.* – The following acts constitute the 18 offenses of cybercrime punishable under this Act:

(A) Offenses against the confidentiality, integrity and availability ofcomputer data and systems:

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

(2) Illegal Interception. - The intentional interception made by
technical means without right of any non-public transmission of computer data
to, from, or within a computer system including electromagnetic emissions
from a computer system carrying such computer data: *Provided*, That it shall
not be unlawful for an officer, employee or agent of a service provider, whose
facilities are used in the transmission of communications, to intercept, disclose,

or use that communication in the normal course of his employment while 1 2 engaged in any activity that is necessary to the rendition of his service or to the 3 protection of the rights or property of the service provider, except that the latter shall not utilize service observing or random monitoring except for 4 5 mechanical or service control quality checks.

6 7

, · ·

(3) Data Interference, - The intentional or reckless alteration of computer data without right.

(4) System Interference. - The intentional or reckless hindering 8 without right of the functioning of a computer system by inputting, 9 10 transmitting, deleting or altering computer data or program.

(5) Misuse of Devices. - (a) The use, production, sale, procurement, 11 importation, distribution or otherwise making available, without right, 12 of: 13

14 (i) A device, including a computer program, designed or adapted 15 primarily for the purpose of committing any of the offenses under this Act; or

16

(ii) A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with the 17 18 intent that it be used for the purpose of committing any of the offenses under 19 this Act.

20 (b) The possession of an item referred to in paragraphs A, 5(a) (i) or 21 (ii) herein with the intent to use said devices for the purpose of committing any 22 of the offenses under this section: Provided. That no criminal liability shall 23 attach when the use, production, sale, procurement, importation, distribution, 24 or otherwise making available, or possession of computer devices/data referred 25 to is for the authorized testing of a computer system.

26

(B) Computer-related Offenses:

(1) Computer Forgery. - (a) The intentional input, alteration or 27 28 deletion of any computer data, without right resulting in unauthentic data with the intent that it be considered or acted upon for legal purposes as if it were
 authentic, regardless whether or not the data is directly readable and
 intelligible; or

4 (b) The act of knowingly using a computer data which is the product of
5 computer-related forgery as defined herein, for the purpose of perpetuating a
6 fraudulent or dishonest design.

7 (2) Computer-related Fraud. – The intentional and unauthorized input, 8 alteration, or deletion of computer data or program or interference in the 9 functioning of a computer system including, but not limited to, phishing, 10 causing damage thereby, with the intent of procuring an economic benefit for 11 oneself or for another person or for the perpetuation of a fraudulent or 12 dishonest activity: *Provided*, That if no damage has yet been caused, the 13 penalty imposable shall be one degree lower.

14

4

.

(C) Content-related Offenses:

15

(1) Cybersex. – Engaging in any of the following acts:

(a) Establishing, maintaining or controlling, directly or indirectly, any
operation for sexual activity or arousal with the aid of or through the use of a
computer system, for a favor or consideration;

(b) Recording private acts including, but not limited to, sexual acts,
without the consent of all parties to the said acts or disseminating any such
recording by any electronic means with or without the consent of all parties to
the said acts;

23 (c) Coercing, intimidating or fraudulently inducing another into doing
24 such indecent acts for exhibition in the internet with the use of computer
25 technologies;

26 (d) Exhibiting live or recorded shows depicting sexual or other obscene27 or indecent acts;

6

2 acts; (f) Establishing, financing, managing, producing or promoting a 3 4 cybersex operation; 5 (g) Participating, in whatever form, in the cybersex operation; and intimidating or inducing anyone to 6 (h) Coercing, threatening, 7 participate in the cybersex operation. 8 (2) Child Pornography. - Engaging in any of the following acts: (a) Producing child pornography for the purpose of distribution 9 10 through a computer system; (b) Offering or making available child pornography through a computer 11 12 system; 13 (c) Distribution or transmitting child pornography through a computer 14 system: (d) Procuring child pornography through a computer system for oneself 15 16 or for another person; or 17 (e) Possessing child pornography materials in the computer system or 18 on a computer data storage device or medium. 19 For the purposes of this section, the term "child pornography" shall 20 include pornographic material that visually depicts: (i) a minor engaged in 21 sexually explicit conduct; (ii) a person appearing to be a minor engaged in 22 sexually explicit conduct; or (iii) realistic images representing a minor engaged 23 in sexually explicit conduct. (3) Unsolicited Commercial Communications. - The transmission of 24 commercial electronic communication with the use of a computer system 25 which seek to advertise, sell or offer for sale products and services are 26

27 prohibited unless:

28

1

(a) There is a prior affirmative consent from the recipient; or

7

(e) Posting of pictures depicting sexual or other obscene or indecent

1

(b) The following conditions are present:

(i) The commercial electronic communication contains a simple, valid 2 3 and reliable way for the recipient to reject receipt of further commercial electronic communication from the same source, also referred to as opt-out; 4

5

(ii) The commercial electronic communication does not purposely disguise the source of the electronic message; and 6

7 (iii) The commercial electronic communication does not purposely 8 include misleading information in any part of the message in order to induce 9 the recipients to read the message.

10 SEC. 5. Other Offenses. - The following acts shall also constitute an 11 offense:

12 (a) Aiding or Abetting in the Commission of Cybercrime. – Any person 13 who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable; or 14

(b) Attempt to Commit Cybercrime. - Any person who willfully 15 attempts to commit any of offenses enumerated in this Act shall be held liable. 16

17 SEC. 6. Liability Under Other Laws. - A prosecution under this Act shall be without prejudice to any liability for violation of any provision of 18 19 Republic Act No. 3815, as amended, otherwise known as the Revised Penal 20 Code, or any other law.

21 22

CHAPTER III

PENALTIES

SEC. 7. Penalties. - The following penalties shall be imposed on 23 24 violations under this Act:

25 (a) Any person found guilty of any of the punishable acts enumerated 26 in Section 4(A) and 4(B) of this Act shall be punished with imprisonment of 27 prision mayor or a fine of at least Two hundred thousand pesos (P200,000.00) 28 up to a maximum amount commensurate to the damage incurred or both;

(b) Any person found guilty of any of the punishable acts enumerated I. 2 in Section 4(C)(1) of this Act shall be punished with imprisonment of prision mayor or a fine of at least Two hundred thousand pesos (P200,000,00) but not 3 4 exceeding One million pesos (P1,000,000.00) or both;

``

5 (c) Any person found guilty of any of the punishable acts enumerated 6 in Section 4(C)(2) of this Act shall be punished with imprisonment of 7 reclusion temporal or a fine of at least Two hundred fifty thousand pesos 8 (P250,000,00) but not exceeding One million two hundred fifty thousand pesos 9 (P1,250,000.00) or both;

10 (d) Any person found guilty of any of the punishable acts enumerated in Section 4(C)(3) shall be punished with imprisonment of arresto mayor or a 11 12 fine of at least Fifty thousand pesos (P50,000.00) but not exceeding Two 13 hundred fifty thousand (P250,000.00) or both; and

14 (e) Any person found guilty of any of the punishable acts enumerated 15 in Section 5 shall be punished with imprisonment one degree lower than that of 16 the prescribed penalty for the offense or a fine of at least One hundred 17 thousand pesos (P100,000.00) but not exceeding Five hundred thousand pesos 18 (P500,000,00) or both.

19 SEC. 8. Corporate Liability. - When any of the punishable acts herein 20 defined is knowingly committed in behalf of or for the benefit of a juridical 21 person, by a natural person acting either individually or as part of an organ of 22 the juridical person, who has a leading position within, based on:

23

28

(a) A power representation of the juridical person:

24 An authority to take decision on behalf of the juridical person; or (b) 25 (c) An authority to exercise control within the juridical person, the 26 27

juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (P10,000,000.00).

1 When the commission of any of the punishable acts herein defined was 2 made possible due to the lack of supervision or control by a natural person 3 referred to and described in the preceding paragraph, for the benefit of that 4 juridical person by a natural person acting under its authority, the juridical 5 person shall be held liable for a fine equivalent to at least double the fines 6 imposable in Section 7 up to a maximum of Five million pesos 7 (P5,000,000.00).

8 The liability imposed on the juridical person shall be without prejudice 9 to the criminal liability of the natural person who has committed the offense.

10

۰.

11

CHAPTER IV

ENFORCEMENT AND IMPLEMENTATION

12 SEC. 9. Law Enforcement Agencies. – The National Bureau of 13 Investigation (NBI) and the Philippine National Police (PNP) shall be 14 responsible for the efficient and effective law enforcement of the provisions of 15 this Act. The NBI and the PNP shall designate special investigators to 16 exclusively handle cases involving violations of this Act.

17 SEC. 10. *Real-time Collection of Computer Data*. – Law enforcement 18 authorities shall be authorized to collect or record by technical or electronic 19 means, and service providers are required to collect or record by technical or 20 electronic means, and/or to cooperate and assist law enforcement authorities in 21 the collection or recording of, traffic data, in real-time, associated with the 22 specified communications transmitted by means of a computer system, subject 23 to existing laws and procedures.

SEC. 11. *Preservation of Computer Data.* – The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved up to a minimum period of six (6) months from the date of the transaction. Content data shall be preserved for a

minimum period of six (6) months from the date of receipt of the order from 1 2 law enforcement authorities requiring its preservation.

3

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

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

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

18 SEC. 13. Search, Seizure and Examination of Computer Data. – Where 19 a search and seizure warrant is properly issued, law enforcement authorities 20 shall, within the time period specified in the warrant, have the following 21 powers and duties:

22

(a) To conduct interception, as defined in this Act, of content data;

23

(b) To secure a computer system or a computer data storage medium;

- (c) To make and retain a copy of secured computer data; 24
- 25

(d) To maintain the integrity of the relevant stored computer data;

26 (e) To conduct examination of the computer data storage medium; and

27 (f) To render inaccessible or remove those computer data in the 28 accessed computer system.

1 The law enforcement authorities may order any person who has 2 knowledge about the functioning of the computer system and the measures to 3 protect and preserve the computer data therein to provide, as is reasonable, the 4 necessary information, to enable the undertaking of the search, seizure and 5 examination.

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

- 10
- 11

CHAPTER V

JURISDICTION

12 SEC. 14. Jurisdiction. - The Regional Trial Court shall have 13 jurisdiction over any violation of the provisions of this Act committed within the territory of the Philippines, including Philippine ships or airships, or by a 14 15 Filipino national regardless of the place of commission. Jurisdiction shall also cover any of the elements committed within the Philippines or committed with 16 17 the use of any computer system wholly or partly situated in the country, or 18 when by such commission, any damage is caused to a natural or juridical 19 person who, at the time the offense was committed, was in the Philippines.

The Department of Justice (DOJ) shall designate special prosecutors to
exclusively handle cases involving violations of this Act.

22 23

CHAPTER VI

INTERNATIONAL COOPERATION

SEC. 15. Mutual Assistance and Cooperation. – The government of the
 Philippines shall cooperate with, and render assistance to other nations for
 purposes of detection, investigation and prosecution of offenses referred to in
 this Act and in the collection of evidence in electronic form in relation thereto.

1 The principles contained in Presidential Decree No. 1069, otherwise known as 2 the Philippine Extradition Law and other pertinent laws shall apply.

3

In this regard, the government of the Philippines shall:

4

(a) Provide assistance to a requesting nation in the real-time collection 5 of traffic data associated with specified communications in the Philippine 6 territory transmitted by means of a computer system, with respect to criminal 7 offenses defined in this Act for which real-time collection of traffic data would 8 be available;

9 (b) Provide assistance to a requesting nation in the real-time collection, 10 recording or interception of content data of specified communications 11 transmitted by means of a computer system to the extent permitted under 12 Republic Act No. 4200, otherwise known as the "Anti-Wiretapping Act", 13 Republic Act No. 9372, otherwise known as the "Human Security Act of 14 2007", and other related and pertinent laws;

15

(c) Allow another nation, without its authorization to:

16 (1) Access publicly available stored computer data, located in 17 Philippine territory, or elsewhere; or

18 (2) Access or receive, through a computer system located in Philippine 19 territory, stored computer data located in another country, if the nation obtains 20 the lawful and voluntary consent of the person who has the lawful authority to 21 disclose the data to the nation through that computer system;

22 (d) Entertain a request of another nation for it to order or obtain the expeditious preservation of data stored by means of a computer system, located 23 24 within Philippine territory, relative to which the requesting nation intends to 25 submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data: 26

27

(1) A request for preservation of data under this section shall specify:

- 28
- (i) The authority seeking the preservation:

1 (ii) The offense that is the subject of a criminal investigation or 2 proceedings and a brief summary of the related facts;

14

~

.

3 (iii) The stored computer data to be preserved and its relationship to4 the offense;

5

(iv) The necessity of the preservation; and

6 (v) That the requesting nation intends to submit a request for mutual 7 assistance for the search or similar access, seizure or similar securing, or 8 disclosure of the stored computer data.

9 (2) Upon receiving the request from another nation, the government of 10 the Philippines shall take all appropriate measures to preserve expeditiously the 11 specified data in accordance with this Act and other pertinent laws. For the 12 purposes of responding to a request, dual criminality shall not be required as a 13 condition to providing such preservation;

14

٩,

(3) A request for preservation may only be refused if:

(i) The request concerns an offense which the government of the
Philippines considers as a political offense or an offense connected with a
political offense; or

18 (ii) The government of the Philippines considers the execution of the
19 request will prejudice its sovereignty, security, public order or other national
20 interest.

(4) Where the government of the Philippines believes that preservation will not ensure the future availability of the data, or will threaten the confidentiality of, or otherwise prejudice the requesting nation's investigation, it shall promptly so inform the requesting nation. The requesting nation will determine whether its request should be executed; and

26 (5) Any preservation effected in response to the request referred to in
27 paragraph (a) shall be for a period not less than sixty (60) days, in order to
28 enable the requesting nation to submit a request for the search or similar access,

•

seizure or similar securing, or disclosure of the data. Following the receipt of 1 2 such a request, the data shall continue to be preserved pending a decision on 3 that request.

4

(e) Accommodate request from another nation to search, access, seize, 5 secure, or disclose data stored by means of a computer system located within 6 Philippine territory, including data that has been preserved under the previous 7 subsection. The government of the Philippines shall respond to the request 8 through the proper application of international instruments, arrangements and 9 laws:

10

(1) The request shall be responded to on an expedited basis where:

11 (i) There are grounds to believe that relevant data is particularly 12 vulnerable to loss or modification; or

13 (ii) The instruments, arrangements and laws referred to in paragraph (b) 14 of this section otherwise provide for expedited cooperation.

15 (2) The requesting nation must maintain the confidentiality of the fact 16 or the subject of request for assistance and cooperation. It may only use the 17 requested information subject to the conditions specified in the grant.

18 SEC. 16. Grounds for Refusal to Cooperate. - The government of the 19 Philippines shall have the right to refuse cooperation under any of the 20 following grounds:

(a) The offense is punishable under Philippine laws and the Philippine 21 22 courts have acquired jurisdiction over the person of the accused;

23

(b) The information requested is privileged, protected under Philippine 24 laws, or that which affects national security;

25 (c) If, for any reason, the production of the information is 26 unreasonable:

1 (d) The foreign government requesting for assistance has previously 2 refused without justifiable reason, a similar request by the government of the 3 Philippines; and

4 (e) The foreign government requesting for assistance has previously 5 breached an agreement to keep the fact or subject of request confidential, or 6 has previously violated any condition of the grant.

7

2.5 .

٠

SEC. 17. Cooperation Based on Reciprocity. - In the absence of a 8 treaty or agreement, mutual assistance and cooperation under the preceding 9 sections in this Chapter shall be based on the principle of reciprocity.

10

11

CHAPTER VII

CYBERCRIME INVESTIGATION AND COORDINATING CENTER

12 SEC. 18. Cybercrime Investigation and Coordinating Center. - There 13 is hereby created, within thirty (30) days from the effectivity of this Act, a 14 Cybercrime Investigation and Coordinating Center, hereinafter referred to as 15 the CICC, under the control and supervision of the Office of the President, to 16 formulate and implement the national cyber security plan.

17 SEC. 19. Composition. - The CICC shall be headed by the Chairman of the Commission on Information and Communications Technology as 18 19 Chairman with the Director of the NBI as Vice Chairman; the Chief of the 20 PNP, the Chief of the National Prosecution Service (NPS) and the Head of the 21 National Computer Center (NCC), as members.

22 The CICC shall be manned by a secretariat of selected personnel and 23 representatives from the different participating agencies.

24

SEC. 20. Powers and Functions. - The CICC shall have the following

25 powers and functions:

26 (a) To prepare and implement appropriate and effective measures to 27 prevent and suppress cybercrime activities as provided for in this Act;

1	(b) To monitor cybercrime cases being handled by participating law
2	enforcement and prosecution agencies;
3	(c) To facilitate international cooperation on intelligence,
4	investigations, training and capacity building related to cybercrime prevention,
5	suppression and prosecution;
6	(d) To coordinate the support and participation of the business sector,
7	local government units and nongovernment organizations in cybercrime
8	prevention programs and other related projects;
9	(e) To recommend the enactment of appropriate laws, issuances,
10	measures and policies;
11	(f) To call upon any government agency to render assistance in the
12	accomplishment of the CICC's mandated tasks and functions; and
13	(g) To perform such other functions and duties necessary for the proper
14	implementation of this Act.
15	CHAPTER VIII
16	FINAL PROVISIONS
17	SEC. 21. Appropriations The amount necessary to implement the
18	provisions of this Act shall be included in the annual General Appropriations
19	Act.
20	SEC. 22. Implementing Rules and Regulations The CICT and the
21	DOJ shall jointly formulate the necessary rules and regulations for the effective
22	implementation of this Act.
23	SEC. 23. Separability Clause If any provision of this Act is held
24	invalid, the other provisions not affected shall remain in full force and effect.
25	SEC. 24. Repealing Clause All laws, decrees or rules inconsistent
26	with this Act are hereby repealed or modified accordingly. Specifically,
27	Section 33 of Republic Act No. 8792 or the Electronic Commerce Act is
28	hereby modified accordingly.

17

SEC. 25. Effectivity. - This Act shall take effect fifteen (15) days after
 its publication in the Official Gazette or in at least two (2) newspapers of
 general circulation.

Approved,

ŧ