Republic of the Philippines
HOUSE OF REPRESENTATIVES
Quezon City, Metro Manila

FIFTEENTH CONGRESS
Second Regular Session

HOUSE BILL NO. 5808
(In Substitution of House Bill Nos. 85, 167, 364, 383, 511, 1444, 2279, 3376, 4031 and 4162)

Introduced by Representatives Susan A. Yap, Eric Owen G. Singson, Jr., Marcelino R. Teodoro, Gloria M. Macapagal-Arroyo, Diosdado M. Arroyo, Juan Edgardo M. Angara, Carmelo F. Lazatin, Rufus B. Rodriguez, Maximo B. Rodriguez, Jr., Mariano Michael M. Velarde, Irwin C. Tieng, Romeo M. Acop, Bernadette R. Herrera-Dy, Anthony Rolando T. Golez, Jr., Juan Miguel Macapagal-Arroyo, Ma. Amelita A. Calimbas-Villarosa, Antonio A. Del Rosario, Winston Castelo, Eulogio R. Magsaysay, Sigfrido R. Tinga, Roilo S. Golez, Romero Federico S. Quimbo, Mel Senen S. Sarmiento, Cesar V. Sarmiento, Daryl Grace J. Abayon, Tomas V. Apacible, Jerry P. Trenas, Joseph Gilbert F. Violago, Hermilando I. Mandanas, and Ma. Rachel J. Arenas and Ma. Victoria Sy-Alvarado

---

AN ACT
DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE 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. ***Short Title***. – This Act shall be known as the "Cybercrime Prevention Act of 2012".

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, 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 safeguard the integrity of computer and communications systems, networks and database, and the confidentiality, integrity and availability of information and data stored therein, from all forms of misuse, abuse and illegal access by making such conduct punishable under the law. In this light, the State shall adopt sufficient powers to effectively prevent and combat such offenses by facilitating their detection, investigation, arrest and prosecution at both the domestic and international levels, and by providing arrangements for fast and reliable international cooperation.

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 or substance, of an existing computer data or program;

(c) *Communication* refers to the transmission of information through ICT medium, including voice, video and other forms of data;

(d) *Computer data* refers to any representation of facts, information or concepts in a form suitable for processing in a computer system, including any program capable of causing a computer system to perform a function, as well as electronic documents or electronic data messages;

(e) *Computer program* refers to a set of instructions executed by the computer to achieve intended results;

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

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

(h) *Cyber* refers to a computer or a computer network, the electronic medium in which online communication takes place;

(i) *Database* refers to a representation of information, knowledge facts, concepts or instructions which are being prepared, processed or stored or have been prepared, processed or stored in an organized manner and which are intended for use in a computer system;

(j) *Interception* refers to listening to, recording, monitoring or surveillance of the content of communications, including procurement of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring;

(k) *Service provider* refers to any public or private entity that provides technically competent information and communication systems services to end users or any other entity that processes or stores computer data or provides infrastructure on behalf of such communication service or users of such service;

(l) *Subscriber's information* refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

(1) the type of communication service used, the technical provisions taken thereto and the period of service;

(2) the subscriber's identity, postal or geographic address, telephone and other access number, any assigned network address, billing and payment information available on the basis of the service agreement; or

(3) any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement; and

(m) *Traffic data or non-content data* refers to any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration or type of underlying service among others.

CHAPTER II

PUNISHABLE ACTS

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

(A) Offenses against the confidentiality, integrity and availability of computer 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, or with dishonest intent or in relation to a computer system that is connected to another computer system, 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 employment while engaged in any activity that is necessary to the rendition of service or to the protection of the rights or property of the service provider, except that the latter shall not utilize service observing or random monitoring except for mechanical or service control quality checks;

(3) Data Interference. – The intentional or reckless alteration, damaging, deletion deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses;

(4) System Interference. – The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting,

transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses;

(5) Misuse of Devices. –

(a) The use, production, sale, procurement, importation, distribution or otherwise making available intentionally and without right, of:

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

(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 intent that it be used for the purpose of committing any of the offenses under this Act;

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

(B) Computer-related Offenses:

(1) Computer Forgery. – (a) The intentional input, alteration, deletion or suppression 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 (b) The act of knowingly using a computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design;

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

(C) Content-related Offenses:

(1) Cybersex. –includes any form of interactive prostitution and other forms of obscenity through the cyberspace as the primary channel with the use of webcams, by inviting people either here or in other countries to watch men, women and children perform sexual acts;

(2) Unsolicited Commercial Communications. - The transmission of commercial electronic communication with the use of a computer system which seeks to advertise, sell or offer for sale products and services are prohibited unless:

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

(b)The following conditions are present:(i) The commercial electronic communication contains a simple, valid and reliable way for the recipient to reject receipt of further commercial electronic communication from the same source, also referred to as opt-out;(ii) The commercial electronic communication does not purposely disguise the source of the electronic message; and(iii) The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

(3) Cyberthreats. – Threatening the life, security or property of another person, whether natural or juridical, or otherwise committing threats and coercions as defined in the Revised Penal Code and other laws, with the aid of or through the use of a computer system, whether using one's real name or an assumed name; and

(4) Cyberdefamation. – The maligning or besmirching the name or reputation, or intriguing against the honor of another person whether natural or juridical, or otherwise committing libel or slander as defined under the Revised Penal Code and other laws with the aid of or through the use of a computer system, whether using one's real name or an assumed name.

SEC. 5. ***Other Offenses***. – The following acts shall also constitute an offense:

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

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

SEC. 6. ***Liability Under Other Laws***. – A prosecution under this Act shall be without prejudice to any liability for violation of any provision of Act No. 3815, as amended, otherwise known as the Revised Penal Code, Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, and Republic Act No. 9995 or the Anti-Photo and Video Voyeurism Act of 2009, or any other law.

CHAPTER III

PENALTIES

SEC. 7. ***Penalties*****.** – The following penalties shall be imposed on violations under this Act:

(a) Any person found guilty of any of the punishable acts enumerated in Section 4(A) and 4(B) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two

Hundred Thousand Pesos (P200,000.00) up to a maximum amount commensurate to the damage incurred or both;

(b) Any person found guilty of any of the punishable acts enumerated 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 exceeding One Million Pesos (P1,000,000.00) or both;

(c) Any person found guilty of any of the punishable acts enumerated in Section 4(C)(2) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty Thousand Pesos (P50,000.00) but not exceeding Two Hundred Fifty Thousand Pesos (P250,000.00) or both; and

(d) Any person found guilty of any of the punishable acts enumerated in Section 4(C)(3) shall be punished with imprisonment of *prision correccional* or a fine of at least Two Hundred Thousand Pesos (P200,000.00) but not exceeding Four Hundred Thousand Pesos (P400,000.00) or both. Where the penalties and fines provided for in the Revised Penal Code or other laws are higher, such higher penalties and fines shall apply.

(e) Any person found guilty of any of the punishable acts enumerated in Section 4(C)(4) shall be punished with imprisonment of *arresto mayor* or a fine of at least One Hundred Thousand Pesos (P100,000.00) but not exceeding Three Hundred Thousand Pesos (P300,000.00) or both. Where the penalties and fines provided for in the Revised Penal Code or other laws are higher, such higher penalties and fines shall apply.

Were the cyberthreat is coupled with a cyberdefamation as defined in Sections 4(C)(3) and 4(C)(4), the penalty to be imposed on the guilty person shall be *prision mayor* or a fine of at least Five Hundred Thousand Pesos (P500,000.00) but not exceeding One Million Pesos (P1,000,000.00) or both. Where the penalties and fines provided for in the Revised Penal Code or other laws are higher, such higher penalties and fines shall apply.

(f) Any person found guilty of any of the punishable acts enumerated in Section 5 hereof shall be punished with imprisonment one degree lower than that of the prescribed penalty for the offense or a fine of at least One Hundred Thousand Pesos (P100,000.00) but not exceeding Five Hundred Thousand Pesos (P500,000.00) or both.

(g) Any officer, employee, agent or representative of a service provider found guilty of any of the punishable acts found herein by virtue of their position, shall be punished with imprisonment of *prision mayor*, or a fine of at least Five Hundred Thousand Pesos (P500,000.00) but not exceeding One Million Pesos (P1,000,000.00) or both.

(h) Any public official or employee who, by reason of the office, with or without consideration, knowingly commits, conspires in the commission, or knowingly conceals violations of any of the provisions of this Act, shall likewise be principally responsible for the violation and be punished with imprisonment of *prision mayor*, or a fine of at least Five Hundred Thousand Pesos (P500,000.00) but not exceeding One Million Pesos (P1,000,000.00) or both, and shall suffer the additional penalty or permanent disqualification to hold public office.

The foregoing criminal penalties shall be without prejudice to the administrative sanctions which the implementing agency may impose under this Act or under any other laws.

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

(a) a power of representation of the juridical person;

(b) an authority to take decisions on behalf of the juridical person; or

(c) an authority to exercise control within the juridical person.

The juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 hereof up to a maximum of Ten Million Pesos (Php10,000.000,00).

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

The chairperson of the board of directors, the president, the general manager of the corporation, the general partners of a partnership, and the officers and employees directly responsible shall be jointly and severally liable with the firm for the fine imposed therein.

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the chairperson of the board of directors, the president, the general manager of the corporation, the general partners of a partnership, and the officers and employees directly responsible for the commission of the offense.

Should the offense be committed by a foreign corporation licensed to do business in the Philippines, the person or persons directly responsible in the Philippines for the management and operation thereof shall be liable. In addition, its license to do business in the Philippines shall be revoked.

It shall not be a defense for the chairperson of the board of directors, the president or the general manager of the corporation or the general partners of a partnership, or the persons responsible for the management and operation of a foreign corporation licensed to do business in the Philippines that they are unaware of the violation, unless established to the satisfaction of the court that even with the exercise of due diligence and proper supervision, they could not have avoided or prevented the violation.

Any agreement between an officer, partner or any other officer and a corporation or partnership whereby the latter directly or indirectly agrees to assume, satisfy or indemnify, in whole or in part, the fine of civil obligation imposed under this Act of such corporate officer, partner, manager or other officer found guilty of violating this Act, shall be void.

CHAPTER IV

ENFORCEMENT AND IMPLEMENTATION

SEC. 9. ***Law Enforcement Agencies***. – The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

SEC. 10. ***Real-time Collection of Computer Data*****.** – Law enforcement authorities, with due cause, and upon securing a court warrant, shall be authorized to collect or record computer data by technical or electronic means. Service providers are required to collect or record computer data by technical or electronic means, and/or to cooperate and assist law enforcement authorities in the collection or recording of traffic data in real-time, associated with the specified communications transmitted by means of a computer system.

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 law enforcement authorities requiring their preservation. Law enforcement authorities may order a one-time extension of six (6) months: *Provided,* That once computer data preserved, transmitted or stored by a service provider are used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case. The service provider ordered to preserve computer data shall keep confidential the order and its compliance.

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

SEC. 13. ***Search, Seizure and Examination of Computer Data*****.** – Where a search and seizure warrant is properly issued, law enforcement authorities shall have the following powers and duties:

a) Within the time period specified in the warrant, to conduct interception as defined in this Act, of content data either directly, through access and use of computer system, or indirectly, through the use of electronic eavesdropping or tapping devices, in real time or at the same time that the communication is occurring only in cases where there is an immediate threat to life and/or threat to national security;

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

c) To make and retain a copy of secured computer data;

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

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

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

The law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination. Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to return the same but in no case for a period longer than thirty (30) days from date of expiration of the warrant.

SEC. 14. ***Jurisdiction***. – The Regional Trial Court shall have jurisdiction over any violation by any person of the provisions of this Act if any of the elements is committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission, any damage or effect is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

SEC. 15. ***Competent Authority***. – The Department of Justice (DOJ) shall be responsible for extending immediate assistance to investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of electronic evidence of a criminal offense and to otherwise ensure compliance with the provisions of this Act. In this regard, there is hereby created a DOJ Office of Cybercrime for facilitating or directly carrying out the provision of technical advice, preservation of data, collection of evidence, giving legal information and locating suspects and all other cybercrime matters related to investigation and reporting issues.

SEC. 16. ***Cybercrime Investigation and Coordinating Center***. – There is hereby created, within thirty (30) days from the effectivity of this Act, an inter-agency body to be known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President, for policy coordination among concerned agencies and for the formulation and enforcement of the national cyber security plan.

SEC. 17. ***Composition***. **–** The CICC shall be headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO-DOST) as Chairperson; with the Director of the NBI as Vice Chairperson; the Chief of the PNP; the Chief of the National Prosecution Service (NPS) and the Head of the National Computer Center (NCC), as members. The CICC shall be manned by a secretariat of selected existing personnel and representatives from the different participating agencies.

SEC. 18. ***Powers and Functions***. **–** The CICC shall have the following powers and functions:

(a) To formulate a national cyber security plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT);

(b) To coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in this Act;

(c) To monitor cybercrime cases being handled by participating law enforcement and prosecution agencies;

(d) To facilitate international cooperation on intelligence, investigations, training and capacity building related to cybercrime prevention, suppression and prosecution;

(e) To coordinate the support and participation of the business sector, local government units and nongovernment organizations in cybercrime prevention programs and other related projects;

(f) To recommend the enactment of appropriate laws, issuances, measures and policies;

(g) To call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions; and

(h) To perform all other matters related to cybercrime prevention and suppression, including capacity building and such other functions and duties as maybe necessary for the proper implementation of this Act.

CHAPTER V

INTERNATIONAL COOPERATION

SEC. 19. ***General Principles Relating to International Cooperation***. – All relevant international instruments on international cooperation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for purposes of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense shall be given full force and effect.

SEC. 20. ***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 covered under this Act and in the collection of evidence in electronic form in relation thereto. The principles contained in Presidential Decree No. 1069, otherwise known as the Philippine Extradition Law and other pertinent laws shall apply. In this regard, the government of the Philippines shall:

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

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

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

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

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

(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 within Philippine territory, relative to which the requesting nation intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data;

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

(i) The authority seeking the preservation;

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

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

(iv) The necessity of the preservation; and

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

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

(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

(ii) The government of the Philippines considers the execution of the request prejudicial to its sovereignty, security, public order or other national 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

(5) Any preservation effected in response to the request referred to in paragraph (a) shall be for a period not less than sixty (60) days, in order to 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 such a request, the data shall continue to be preserved pending a decision on that request.

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

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

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

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

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

SEC. 21. ***Grounds for Refusal to Cooperate***. – The government of the Philippines shall have the right to refuse cooperation under any of the following grounds:

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

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

(c) If, for any reason, the production of the information is unreasonable;

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

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

SEC. 22. ***Applicability of the Convention*** **on** ***Cybercrime.*** – The provisions of Chapter III on International Cooperation of the Convention on Cybercrime shall be directly applicable in the implementation of this Act taking into account the procedural laws obtaining in the jurisdiction.

SEC. 23. ***Cooperation Based on Reciprocity***. – In the absence of a treaty or agreement, mutual assistance and cooperation under the preceding sections in this Chapter shall be based on the principle of reciprocity.

CHAPTER VI

FINAL PROVISIONS

SEC. 24. ***Appropriations***. – The amount necessary for the initial implementation of this Act shall be charged against the current year's appropriations of the Information and Communications Technology Office. Thereafter, such sums as maybe necessary for the continued implementation of this Act shall be included in the annual General Appropriations Act.

SEC. 25. ***Implementing Rules and Regulations***. – The ICTO-DOST, DOJ and the Department of the Interior and Local Government (DILG) shall jointly formulate the necessary rules and regulations within ninety (90) days from approval of this Act, for its effective implementation.

SEC.26. ***Separability Clause***. – If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

SEC. 27. ***Repealing Clause***. – All laws, decrees, or rules inconsistent with this Act are hereby repealed or modified accordingly. Specifically, Section 33 on Penalties of Republic Act No. 8792 or the Electronic Commerce Act, is hereby modified accordingly.

SEC. 28. ***Effectivity Clause***. – 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,