Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012"

Pursuant to the authority of the Department of Justice, Department of Interior and Local Government, and Department of Science and Technology under Republic Act No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012", the following rules and regulations are hereby promulgated to implement the provisions of said Act:

RULE 1
Preliminary Provisions

Section 1. ***Title.*** – These Rules shall be referred to as the Implementing Rules and Regulations of Republic Act No. 10175, or the "Cybercrime Prevention Act of 2012".

Section 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 State'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.

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.

Section 3. ***Definition of Terms.*** – The following terms are 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) ***Act*** refers to Republic Act No. 10175 or the "Cybercrime Prevention Act of 2012";

c) ***Alteration*** refers to the modification or change, in form or substance, of an existing computer data or program;

d) ***Central Authority*** refers to the DOJ – Office of Cybercrime;

e) ***Child Pornography*** refers to the unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009", committed through a computer system: *Provided,* that the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775;

f) ***Collection*** refers to gathering and receiving information;

g) ***Communication*** refers to the transmission of information through information and communication technology (ICT) media, including voice, video and other forms of data;

h) ***Competent Authority*** refers to either the Cybercrime Investigation and Coordinating Center or the DOJ – Office of Cybercrime, as the case may be;

i) ***Computer*** refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical, arithmetic, routing or storage functions, and which includes any storage facility or equipment or communications facility or equipment directly related to or operating in conjunction with such device. It covers any type of computer device, including devices with data processing capabilities like mobile phones,

smart phones, computer networks and other devices connected to the internet;

j) ***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 whether stored in local computer systems or online;

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

l) ***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 to a network or other similar devices. It also includes computer data storage devices or media;

m) ***Content Data*** refers to the communication content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data.

n) ***Critical infrastructure*** refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data that are so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters;

o) ***Cybersecurity*** refers to the collection of tools, policies, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment, and organization and user's assets;

p) ***National Cybersecurity Plan*** refers to a comprehensive plan of actions designed to improve the security and enhance cyber resilience of infrastructures and services. It is a top-down approach to cybersecurity that

contains broad policy statements and establishes a set of national objectives and priorities that should be achieved within a specific timeframe;

q) ***Cybersex*** refers to the willful engagement, maintenance, control or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration;

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

s) ***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 a formalized manner, and which are intended for use in a computer system;

t) ***Digital evidence*** refers to digital information that may be used as evidence in a case. The gathering of the digital information may be carried out by confiscation of the storage media (data carrier), the tapping or monitoring of network traffic, or the making of digital copies (*e.g.,* forensic images, file copies, etc.), of the data held;

u) ***Electronic evidence*** refers to evidence, the use of which is sanctioned by existing rules of evidence, in ascertaining in a judicial proceeding, the truth respecting a matter of fact, which evidence is received, recorded, transmitted, stored, processed, retrieved or produced electronically;

v) ***Forensics*** refers to the application of investigative and analytical techniques that conform to evidentiary standards, and are used in, or appropriate for, a court of law or other legal context;

w) ***Forensic image***, also known as a ***forensic copy***, refers to an exact bit-by-bit copy of a data carrier, including slack, unallocated space and unused space. There are forensic tools available for making these images. Most tools produce information, like a hash value, to ensure the integrity of the image;

x) ***Hash value*** refers to the mathematical algorithm produced against digital information (a file, a physical disk or a logical disk) thereby creating a "digital fingerprint" or "digital DNA" for that information. It is a one-way

algorithm and thus it is not possible to change digital evidence without changing the corresponding hash values;

y) ***Identifying information*** refers to any name or number that may be used alone or in conjunction with any other information to identify any specific individual, including any of the following:

1. Name, date of birth, driver's license number, passport number or tax identification number;

2. Unique biometric data, such as fingerprint or other unique physical representation;

3. Unique electronic identification number, address or routing code; and

4. Telecommunication identifying information or access device.

z) ***Information and communication technology system*** refers to system intended for, and capable of, generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents, and includes the computer system or other similar device by or in which data is recorded or stored, and any procedures related to the recording or storage of electronic data message or electronic document;

aa) ***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;

bb) ***Internet content host*** refers to a person who hosts or who proposes to host internet content in the Philippines;

cc) ***Law enforcement authorities*** refers to the National Bureau of Investigation (NBI) and the Philippine National Police (PNP) under Section 10 of the Act;

dd) ***Original author*** refers to the person who created or is the origin of the assailed electronic statement or post using a computer system;

ee) ***Preservation*** refers to the keeping of data that already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate. It is the activity that keeps that stored data secure and safe;

ff) ***Service provider*** refers to:

1. any public or private entity that provides users of its service with the ability to communicate by means of a computer system; and

2. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

gg) ***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 any of the following 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 that are available on the basis of the service agreement or arrangement; or

3. Any other available information on the site of the installation of communication equipment that is available on the basis of the service agreement or arrangement.

hh) ***Traffic Data or Non-Content Data*** refers to any computer data other than the content of the communication, including, but not limited to the communication's origin, destination, route, time, date, size, duration, or type of underlying service; and

ii) ***Without Right*** refers to either: (i) 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.

RULE 2
Punishable Acts and Penalties

Cybercrimes

Section 4. ***Cybercrime Offenses.*** – The following acts constitute the offense of core cybercrime punishable under the Act:

A. **Offenses against the confidentiality, integrity and availability of computer data and systems** shall be punished with imprisonment of *prision mayor* or a fine of at least Two Hundred Thousand Pesos (₱200,000.00) up to a maximum amount commensurate to the damage incurred, or both, except with respect to number 5 herein:

1. **Illegal Access** – The access to the whole or any part of a computer system without right.

2. **Illegal Interception** – The interception made by technical means and 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, however*, 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 other than for purposes of mechanical or service control quality checks.

3. **Data Interference** – The intentional or reckless alteration, damaging, deletion or 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**, which shall be punished with imprisonment of *prision mayor,* or a fine of not more than Five Hundred Thousand Pesos (₱500,000.00), or both, is committed through any of the following acts:

   a. The use, production, sale, procurement, importation, distribution or otherwise making available, intentionally and without right, of any of the following:

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

   b. The possession of an item referred to in subparagraphs 5(a)(i) or (ii) above, with the intent to use said devices for the purpose of committing any of the offenses under this section.

   Provided, That no criminal liability shall attach when the use, production, sale, procurement, importation, distribution, otherwise making available, or possession of computer devices or data referred to in this section is for the authorized testing of a computer system.

If any of the punishable acts enumerated in Section 4(A) is committed against critical infrastructure, the penalty of *reclusion temporal*, or a fine of at least Five Hundred Thousand Pesos (₱500,000.00) up to maximum amount commensurate to the damage incurred, or both shall be imposed.

B. **Computer-related Offenses**, which shall be punished with imprisonment of *prision mayor*, or a fine of at least Two Hundred Thousand Pesos (₱200,000.00) up to a maximum amount commensurate to the damage incurred, or both, are as follows:

1. **Computer-related Forgery** –

   a. The input, alteration or deletion of any computer data without right, resulting in inauthentic 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 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 unauthorized input, alteration or deletion of computer data or program, or interference in the functioning of a computer system, causing damage thereby with fraudulent intent: *Provided,* That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

3. **Computer-related Identity Theft** – The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical, without right: *Provided,* That if no damage has yet been caused, the penalty imposable shall be one (1) degree lower.

C. **Content-related Offenses**:

1. Any person found guilty of Child Pornography shall be punished in accordance with the penalties set forth in Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009": *Provided,* That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775 if committed through a computer system.

Section 5. ***Other Cybercrimes.*** – The following constitute other cybercrime offenses punishable under the Act:

1. **Cyber-squatting** – The acquisition of a domain name over the internet, in bad faith, in order to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

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

b. Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and

c. Acquired without right or with intellectual property interests in it.

Cyber-squatting shall be punished with imprisonment of *prision mayor*, or a fine of at least Two Hundred Thousand Pesos (₱200,000.00) up to a maximum amount commensurate to the damage incurred, or both: *Provided,* That if it is committed against critical infrastructure, the penalty of *reclusion temporal*, or a fine of at least Five Hundred Thousand Pesos (₱500,000.00) up to maximum amount commensurate to the damage incurred, or both shall be imposed.

2. **Cybersex** – The willful engagement, maintenance, control or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration. Any person found guilty cybersex shall be punished with imprisonment of *prision mayor*, or a fine of at least Two Hundred Thousand Pesos (₱200,000.00), but not exceeding One Million Pesos (₱1,000,000.00), or both.

   Cybersex involving a child shall be punished in accordance with the provision on child pornography of the Act.

   Where the maintenance, control, or operation of cybersex likewise constitutes an offense punishable under Republic Act No. 9208, as amended, a prosecution under the Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws, including R.A. No. 9208, consistent with Section 8 hereof.

3. **Libel** – The unlawful or prohibited acts of libel, as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future shall be punished with *prision correccional* in its maximum period to *prision mayor* in its minimum period or a fine ranging from Six

Thousand Pesos (₱6,000.00) up to the maximum amount determined by Court, or both, in addition to the civil action which may be brought by the offended party: *Provided,* That this provision applies only to the original author of the post or online libel, and not to others who simply receive the post and react to it.

4. **Other offenses** – The following acts shall also constitute an offense which shall be punished with imprisonment of one (1) degree lower than that of the prescribed penalty for the offense, or a fine of at least One Hundred Thousand Pesos (₱100,000.00) but not exceeding Five Hundred Thousand Pesos (₱500,000.00), or both:

   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 the Act shall be held liable, except with respect to Sections 4(c)(2) on Child Pornography and 4(c)(4) on online Libel.

   B. Attempt to Commit Cybercrime. – Any person who willfully attempts to commit any of the offenses enumerated in the Act shall be held liable, except with respect to Sections 4(c)(2) on Child Pornography and 4(c)(4) on online Libel.

Other Liabilities and Penalties

Section 6. ***Corporate Liability.*** – When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, 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 up to a maximum of Ten Million Pesos (₱10,000,000.00).

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 referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the 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 Five Million Pesos (₱5,000,000.00).

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

Section 7. ***Violation of the Revised Penal Code, as Amended, Through and With the Use of Information and Communication Technology.*** – All crimes defined and penalized by the Revised Penal Code, as amended, and special criminal laws committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of the Act: *Provided,* That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

Section 8. ***Liability under Other Laws.*** – A prosecution under the Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws: *Provided*, That this provision shall not apply to the prosecution of an offender under (1) both Section 4(c)(4) of R.A. 10175 and Article 353 of the Revised Penal Code; and (2) both Section 4(c)(2) of R.A. 10175 and R.A. 9775 or the "Anti-Child Pornography Act of 2009".

RULE 3
Enforcement and Implementation

Section 9. ***Law Enforcement Authorities.*** – 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 the Act. The NBI and the PNP shall organize a cybercrime division or unit to be manned by Special Investigators to exclusively handle cases involving violations of the Act.

The NBI shall create a cybercrime division to be headed by at least a Head Agent. The PNP shall create an anti-cybercrime unit headed by at least a Police Director.

The DOJ - Office of Cybercrime (OOC) created under the Act shall coordinate the efforts of the NBI and the PNP in enforcing the provisions of the Act.

Section 10. ***Powers and Functions of Law Enforcement Authorities.*** – The NBI and PNP cybercrime unit or division shall have the following powers and functions:

a. Investigate all cybercrimes where computer systems are involved;

b. Conduct data recovery and forensic analysis on computer systems and other electronic evidence seized;

c. Formulate guidelines in investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices;

d. Provide technological support to investigating units within the PNP and NBI including the search, seizure, evidence preservation and forensic recovery of data from crime scenes and systems used in crimes, and provide testimonies;

e. Develop public, private sector, and law enforcement agency relations in addressing cybercrimes;

f. Maintain necessary and relevant databases for statistical and/or monitoring purposes;

g. Develop capacity within their organizations in order to perform such duties necessary for the enforcement of the Act;

h. Support the formulation and enforcement of the national cybersecurity plan; and

i. Perform other functions as may be required by the Act.

Section 11. ***Duties of Law Enforcement Authorities.*** – To ensure that the technical nature of cybercrime and its prevention is given focus, and considering the procedures involved for international cooperation, law enforcement authorities, specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes, are required to submit timely and regular reports including pre-operation, post-operation and investigation results, and such other documents as may be required to the Department of Justice (DOJ) – Office of Cybercrime for review and monitoring.

Law enforcement authorities shall act in accordance with the guidelines, advisories and procedures issued and promulgated by the competent authority in all matters related to cybercrime, and utilize the prescribed forms and templates, including, but not limited to, preservation orders, chain of custody, consent to search, consent to assume account/online identity and request for computer forensic examination.

Section 12. ***Preservation and Retention of Computer Data.*** – The integrity of traffic data and subscriber information shall be kept, retained and preserved by a service provider for a minimum period of six (6) months from the date of the transaction. Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one-time extension for another six (6) months: *Provided*, That once computer data that is preserved, transmitted or stored by a service provider is used as evidence in a case, the mere act of furnishing such service provider with a copy of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the final termination of the case and/or as ordered by the Court, as the case may be.

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

Section 13. ***Collection of Computer Data.*** Law enforcement authorities, upon the issuance of a court warrant, shall be authorized to collect or record by technical or electronic means, and the service providers are required to collect or record by technical or electronic means and/or to cooperate and assist in the collection or recording of computer data that are associated with specified communications transmitted by means of a computer system.

The court warrant required under this section shall be issued or granted upon written application, after the examination under oath or affirmation of the applicant and the witnesses he may produce, and the showing that: (1) there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, is being committed or is about to be committed; (2) there are reasonable grounds to believe that the evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of any

such crimes; and (3) there are no other means readily available for obtaining such evidence.

Section 14. ***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, within seventy-two (72) hours from receipt of such order, subscriber's information, traffic data or relevant data in his/its possession or control, in relation to a valid complaint officially docketed and assigned for investigation by law enforcement authorities, and the disclosure of which is necessary and relevant for the purpose of investigation.

Law enforcement authorities shall record all sworn complaints in their official docketing system for investigation.

Section 15. ***Search, Seizure and Examination of Computer Data.*** – Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties:

a. Within the time period specified in the warrant, to conduct interception, as defined in this Rules, and to:

    1. Search and seize computer data;

    2. Secure a computer system or a computer data storage medium;

    3. Make and retain a copy of those computer data secured;

    4. Maintain the integrity of the relevant stored computer data;

    5. Conduct forensic analysis or examination of the computer data storage medium; and

    6. Render inaccessible or remove those computer data in the accessed computer or computer and communications network.

b. Pursuant thereto, 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.

c. 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 approval by the court.

Section 16. ***Custody of Computer Data.*** – All computer data, including content and traffic data, that are examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it, stating the dates and times covered by the examination, and the law enforcement authority who may have access to the deposit, among other relevant data. The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made or, if made, that all such duplicates or copies are included in the package deposited with the court. The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or their contents revealed, except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.

Section 17. ***Destruction of Computer Data.*** – Upon expiration of the periods as provided in Sections 12 and 15 hereof, or until the final termination of the case and/or as ordered by the Court, as the case may be, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data that are the subject of a preservation and examination order or warrant.

Section 18. ***Exclusionary Rule.*** – Any evidence obtained without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

The Rules of Court shall have suppletory application in implementing the Act.

Section 19. ***Non-compliance.*** – Failure to comply with the provisions of Chapter IV of the Act, and Rules 7 and 8 of Chapter VII hereof, specifically the orders from law enforcement authorities, shall be punished as a violation of Presidential Order No. 1829 (entitled "*Penalizing Obstruction Of Apprehension And Prosecution Of Criminal Offenders*") with imprisonment of *prision correccional* in its maximum period, or a fine of One Hundred Thousand Pesos (₱100,000.00), or both for each and every noncompliance with an order issued by law enforcement authorities.

Section 20. ***Extent of Liability of a Service Provider.*** – Except as otherwise provided in this Section, no person or party shall be subject to any civil or criminal liability in respect of a computer data for which the person or party acting as a service provider merely provides access if such liability is founded on:

a. The obligations and liabilities of the parties under a computer data;

b. The making, publication, dissemination or distribution of such computer data or any statement made in such computer data, including possible infringement of any right subsisting in or in relation to such computer data: *Provided*, That:

   1. The service provider does not have actual knowledge, or is not aware of the facts or circumstances from which it is apparent, that the making, publication, dissemination or distribution of such material is unlawful or infringes any rights subsisting in or in relation to such material;

   2. The service provider does not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity; and

   3. The service provider does not directly commit any infringement or other unlawful act, does not induce or cause another person or party to commit any infringement or other unlawful act, and/or does not directly benefit financially from the infringing activity or unlawful act of another person or party: *Provided, further*, That nothing in this Section shall affect:

      i. Any obligation arising from contract;

ii. The obligation of a service provider as such under a licensing or other regulatory regime established under law;

iii. Any obligation imposed under any law; or

iv. The civil liability of any party to the extent that such liability forms the basis for injunctive relief issued by a court under any law requiring that the service provider take or refrain from actions necessary to remove, block or deny access to any computer data, or to preserve evidence of a violation of law.

RULE 4
Jurisdiction

Section 21. ***Jurisdiction.*** – The Regional Trial Court shall have jurisdiction over any violation of the provisions of the Act, including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines, or committed with the use of any computer system that is wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

Section 22. ***Venue.*** – Criminal action for violation of the Act may be filed with the RTC of the province or city where the cybercrime or any of its elements is committed, or where any part of the computer system used is situated, or where any of the damage caused to a natural or juridical person took place: *Provided,* That the court where the criminal action is first filed shall acquire jurisdiction to the exclusion of other courts.

Section 23. ***Designation of Cybercrime Courts.*** – There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

Section 24. ***Designation of Special Prosecutors and Investigators.*** – The Secretary of Justice shall designate prosecutors and investigators who shall

comprise the prosecution task force or division under the DOJ-Office of Cybercrime, which will handle cybercrime cases in violation of the Act.

RULE 5
International Cooperation

Section 25. ***International Cooperation.*** – All relevant international instruments on international cooperation on criminal matters, and arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws shall be given full force and effect, to the widest extent possible for the purposes of investigations or proceedings concerning crimes related to computer systems and data, or for the collection of electronic evidence of crimes.

The DOJ shall cooperate and render assistance to other contracting parties, as well as request assistance from foreign states, for purposes of detection, investigation and prosecution of offenses referred to in the Act and in the collection of evidence in electronic form in relation thereto. The principles contained in Presidential Decree No. 1069 and other pertinent laws, as well as existing extradition and mutual legal assistance treaties, shall apply. In this regard, the central authority shall:

a. Provide assistance to a requesting State in the real-time collection of traffic data associated with specified communications in the country transmitted by means of a computer system, with respect to criminal offenses defined in the Act for which real-time collection of traffic data would be available, subject to the provisions of Section 13 hereof;

b. Provide assistance to a requesting State in the real-time collection, recording or interception of content data of specified communications transmitted by means of a computer system, subject to the provision of Section 13 hereof;

c. Allow another State to:

    1. Access publicly available stored computer data located in the country or elsewhere; or

    2. Access or receive, through a computer system located in the country, stored computer data located in another country, if the other State obtains the lawful and voluntary consent of the person who has the lawful

authority to disclose the data to said other State through that computer system.

d. Receive a request of another State for it to order or obtain the expeditious preservation of data stored by means of a computer system located within the country, relative to which the requesting State shall submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data: *Provided*, That:

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 State shall 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 State, the DOJ and law enforcement agencies shall take all appropriate measures to expeditiously preserve the specified data, in accordance with the Act and other pertinent laws. For the purposes of responding to a request for preservation, dual criminality shall not be required as a condition;

3. A request for preservation may only be refused if:

   i. The request concerns an offense that the Philippine Government considers as a political offense or an offense connected with a political offense; or

   ii. The Philippine Government considers the execution of the request to be prejudicial to its sovereignty, security, public order or other national interest.

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

5. Any preservation effected in response to the request referred to in paragraph (d) shall be for a period not less than sixty (60) days, in order to enable the requesting State 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 request from another State to search, access, seize, secure, or disclose data stored by means of a computer system located within the country, including data that has been preserved under the previous subsection.

The Philippine Government shall respond to the request through the proper application of international instruments, arrangements and laws, and in accordance with the following rules:

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 State must maintain the confidentiality of the fact or the subject of request for assistance and cooperation. It may only use the requested information subject to the conditions specified in the grant.

f. Make a request to any foreign state for assistance for purposes of detection, investigation and prosecution of offenses referred to in the Act;

g. The criminal offenses described under Chapter II of the Act shall be deemed to be included as extraditable offenses in any extradition treaty where the Philippines is a party: *Provided*, That the offense is punishable under the laws of both Parties concerned by deprivation of liberty for a minimum period of at least one year or by a more severe penalty.

The Secretary of Justice shall designate appropriate State Counsels to handle all matters of international cooperation as provided in this Rule.

RULE 6
Competent Authorities

Section 26. ***Cybercrime Investigation and Coordinating Center; Composition.*** – The inter-agency body known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President, established for policy coordination among concerned agencies and for the formulation and enforcement of the national cyber security plan, is headed by the Executive Director of the Information and Communications Technology Office under the Department of Science and Technology (ICTO-DOST) as Chairperson; the Director of the NBI as Vice-Chairperson; and the Chief of the PNP, the Head of the DOJ Office of Cybercrime, and one (1) representative each from the private sector, non-governmental organizations, and the academe as members.

The CICC members shall be constituted as an Executive Committee and shall be supported by Secretariats, specifically for Cybercrime, Administration, and Cybersecurity. The Secretariats shall be manned from existing personnel or representatives of the participating agencies of the CICC.

The CICC may enlist the assistance of any other agency of the government including government-owned and -controlled corporations, and the following:

a. Bureau of Immigration;

b. Philippine Drug Enforcement Agency;

c. Bureau of Customs;

d. National Prosecution Service;

e. Anti-Money Laundering Council;

f. Securities and Exchange Commission;

g. National Telecommunications Commission; and

h. Such other offices, agencies and/or units, as may be necessary.

The DOJ Office of Cybercrime shall serve as the Cybercrime Operations Center of the CICC and shall submit periodic reports to the CICC.

Participation and representation in the Secretariat and/or Operations Center does not require physical presence, but may be done through electronic modes such as email, audio-visual conference calls, and the like.

Section 27. ***Powers and Functions.*** – The CICC shall have the following powers and functions:

a. Formulate a national cybersecurity plan and extend immediate assistance for the suppression of real-time commission of cybercrime offenses through a computer emergency response team (CERT);

b. Coordinate the preparation of appropriate and effective measures to prevent and suppress cybercrime activities as provided for in the Act;

c. Monitor cybercrime cases being handled by participating law enforcement and prosecution agencies;

d. Facilitate international cooperation on intelligence, investigations, training and capacity-building related to cybercrime prevention, suppression and prosecution through the DOJ-Office of Cybercrime;

e. Coordinate the support and participation of the business sector, local government units and NGOs in cybercrime prevention programs and other related projects;

f. Recommend the enactment of appropriate laws, issuances, measures and policies;

g. Call upon any government agency to render assistance in the accomplishment of the CICC's mandated tasks and functions;

h. Establish and perform community awareness program on cybercrime prevention in coordination with law enforcement authorities and stakeholders; and

i. Perform all other matters related to cybercrime prevention and suppression, including capacity-building and such other functions and duties as may be necessary for the proper implementation of the Act.

Section 28. ***Department of Justice (DOJ); Functions and Duties.*** – The DOJ-Office of Cybercrime (OOC), designated as the central authority in all matters related to international mutual assistance and extradition, and the Cybercrime Operations Center of the CICC, shall have the following functions and duties:

a. Act as a competent authority for all requests for assistance for investigation or proceedings concerning cybercrimes, facilitate the provisions of legal or technical advice, preservation and production of data, collection of evidence, giving legal information and location of suspects;

b. Act on complaints/referrals, and cause the investigation and prosecution of cybercrimes and other violations of the Act;

c. Issue preservation orders addressed to service providers;

d. Administer oaths, issue subpoena and summon witnesses to appear in an investigation or proceedings for cybercrime;

e. Require the submission of timely and regular reports including pre-operation, post-operation and investigation results, and such other documents from the PNP and NBI for monitoring and review;

f. Monitor the compliance of the service providers with the provisions of Chapter IV of the Act, and Rules 7 and 8 hereof;

g. Facilitate international cooperation with other law enforcement agencies on intelligence, investigations, training and capacity-building related to cybercrime prevention, suppression and prosecution;

h. Issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices;

i. Prescribe forms and templates, including, but not limited to, those for preservation orders, chain of custody, consent to search, consent to assume account/online identity, and request for computer forensic examination;

j. Undertake the specific roles and responsibilities of the DOJ related to cybercrime under the Implementing Rules and Regulation of Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009"; and

k. Perform such other acts necessary for the implementation of the Act.

Section 29. ***Computer Emergency Response Team (CERT).*** – The DOST-ICT Office shall establish and operate the Computer Emergency Response Team (CERT) that shall serve as coordinator for cybersecurity related activities, including but not limited to the following functions and duties:

a. Extend immediate assistance to the CICC to fulfil its mandate under the Act with respect to matters related to cybersecurity and the national cybersecurity plan;

b. Issue and promulgate guidelines, advisories, and procedures in all matters related to cybersecurity and the national cybersecurity plan;

c. Facilitate international cooperation with other security agencies on intelligence, training, and capacity-building related to cybersecurity; and

d. Serve as the focal point for all instances of cybersecurity incidents by:

   1. Providing technical analysis of computer security incidents;

2. Assisting users in escalating abuse reports to relevant parties;

3. Conducting research and development on emerging threats to computer security;

4. Issuing relevant alerts and advisories on emerging threats to computer security.

5. Coordinating cyber security incident responses with trusted third parties at the national and international levels; and

6. Conducting technical training on cyber security and related topics.

The Philippine National Police and the National Bureau of Investigation shall serve as the field operations arm of the CERT. The CERT may also enlist other government agencies to perform CERT functions.

RULE 7
Duties of Service Providers

Section 30. ***Duties of a Service Provider.*** – The following are the duties of a service provider:

a. Preserve the integrity of traffic data and subscriber information for a minimum period of six (6) months from the date of the transaction;

b. Preserve the integrity of content data for six (6) months from the date of receipt of the order from law enforcement or competent authorities requiring its preservation;

c. Preserve the integrity of computer data for an extended period of six (6) months from the date of receipt of the order from law enforcement or competent authorities requiring extension on its preservation;

d. Preserve the integrity of computer data until the final termination of the case and/or as ordered by the Court, as the case may be, upon receipt of a copy of the transmittal document to the Office of the Prosecutor;

e. Ensure the confidentiality of the preservation orders and its compliance;

f. Collect or record by technical or electronic means, and/or cooperate and assist law enforcement or competent authorities in the collection or recording of computer data that are associated with specified communications transmitted by means of a computer system, in relation to Section 13 hereof;

g. Disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control to law enforcement or competent authorities within seventy-two (72) hours after receipt of order and/or copy of the court warrant;

h. Report to the DOJ – Office of Cybercrime compliance with the provisions of Chapter IV of the Act, and Rules 7 and 8 hereof;

i. Immediately and completely destroy the computer data subject of a preservation and examination after the expiration of the period provided in Sections 13 and 15 of the Act; and

j. Perform such other duties as may be necessary and proper to carry into effect the provisions of the Act.

Section 31. ***Duties of a Service Provider in Child Pornography Cases.*** – In line with RA9775 or the "Anti-Child Pornography Act of 2009", the following are the duties of a service provider in child pornography cases:

1. An internet service provider (ISP)/internet content host shall install available technology, program or software, such as, but not limited to, system/technology that produces hash value or any similar calculation, to ensure that access to or transmittal of any form of child pornography will be blocked or filtered;

2. Service providers shall immediately notify law enforcement authorities within seven (7) days of facts and circumstances relating to any form child pornography that passes through or are being committed in their system; and

3. A service provider or any person in possession of traffic data or subscriber's information, shall, upon the request of law enforcement or competent authorities, furnish the particulars of users who gained or

attempted to gain access to an internet address that contains any form of child pornography. ISPs shall also preserve customer data records, specifically the time, origin, and destination of access, for purposes of investigation and prosecution by relevant authorities under Sections 9 and 11 of R.A. 9775.

RULE 8
Prescribed Forms and Procedures

SEC. 32. ***Prescribed Forms and Procedures.*** — The DOJ – Office of Cybercrime shall issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime, investigation, forensic evidence recovery, and forensic data analysis consistent with international best practices, in accordance with Section 28(h) and (i) hereof.

It shall also prescribe forms and templates such as, but not limited to, preservation orders, chain of custody, consent to search, consent to assume account/online identity, request for computer forensic assistance, write-blocking device validation and first responder checklist.

RULE 9
Final Provisions

SEC. 33. ***Appropriations.*** — The amount of Fifty Million Pesos (₱50,000,000.00) shall be appropriated annually for the implementation of the Act under the fiscal management of DOJ - Office of Cybercrime.

Section 34. ***Separability Clause.*** – If any provision of these Rules is held invalid, the other provisions not affected shall remain in full force and effect.

Section 35. ***Repealing Clause.*** – All rules and regulations inconsistent with these Rules are hereby repealed or modified accordingly.

Section 36. ***Effectivity.*** – These rules and regulations shall take effect fifteen (15) days after the completion of its publication in at least two (2) newspapers of general circulation.

DONE in the City of Manila, this 12th day of August 2015.

MAR ROXAS
Secretary
Department of Interior and Local Government

MARIO G. MONTEJO
Secretary
Department of Science and Technology

LEILA M. DE LIMA
Secretary
Department of Justice