SEVENTEENTH CONGRESS
OF THE REPUBLIC OF THE PHILIPPINES
First Regular Section

HOUSE OF REPRESENTATIVES
RECEIVED
17 AUG 2016
DATE:
TIME:
BY:
REGISTRATION UNIT
BILLS AND INDEX SERVICE

House Bill No. 3056

Introduced by Representative Victor A. Yap

EXPLANATORY NOTE

As far back as 2001, analyst Doug Laney articulated the now mainstream definition of big data as the three Vs of big data: volume, velocity and variety.

> Volume. Many factors contribute to the increase in data volume. Transaction-based data stored through the years. Unstructured data streaming in from social media. Increasing amounts of sensor and machine-to-machine data being collected.
>
> Velocity. Data is streaming in at unprecedented speed and must be dealt with in a timely manner. RFID tags, sensors and smart metering are driving the need to deal with torrents of data in near-real time. Reacting quickly enough to deal with data velocity is a challenge.
>
> Variety. Data today comes in all types of formats. Structured, numeric data in traditional databases. Information created from line-of-business applications. Unstructured text documents, email, video, audio, stock ticker data and financial transactions. Managing, merging and governing different varieties of data is something difficult to grapple with.

This measure seeks to establish the Philippine Big Data Center (Center) to facilitate the handling and processing of big data with a focus on making policy and services to be more responsive to public needs and welfare- this is a true step forward in realizing the welfare of the people as the supreme law.

The analysis of big data will be beneficial in multiple issue areas that involve complex and voluminous data sets- disaster risk management in particular can benefit, likewise research and development as well as innovation and invention, and similarly policy making.

By developing standards for software and tools in analytics, the Center is envisioned to be capable of generating invaluable research and information for a multiplicity of users, as well as the general public.

The Center is an important step forward and investment for governance and scientific and technological development. We acknowledge that Sen. Paolo Benigno "Bam" Aquino filed this proposed measured in the Senate.

Hence, the bill is urgent and ought to be passed.

VICTOR A. YAP
Representative, 2nd District of Tarlac

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

HOUSE OF REPRESENTATIVES

House Bill No. _____

Introduced by Representative Victor A. Yap

AN ACT INSTITUTIONALIZING THE ESTABLISHMENT OF THE PHILIPPINE BIG DATA CENTER

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

SECTION 1. ***Title.*** - This Act shall be known as the "*Big Data Act*".

SEC. 2. ***Declaration of Policy.*** - The State recognizes the vital role of communication and information in nation-building. Access to official records, and to documents and papers pertaining to official acts, transactions, or decisions as well as to government research data as basis for policy development, shall be afforded the citizen, subject to such limitations as may be provided by law. Further, the State also recognizes that science and technology are essential for national development and progress. The State shall give priority to research and development, invention, innovation, and their utilization; and to science and technology education, training, and services.

In line with these basic constitutional guarantees it shall be the policy of the state to revolutionize government's efforts in promoting and maintaining an efficient government statistical system that provides adequate, accessible, consistent, reliable and timely data. The establishment of the Big Data Center shall also ensure that existing government data are also maximized as supported by the Open Data Philippines program pursuant to E.O. 43 or the overall governance framework.

The Big Data Center shall pave the way that will allow our country to make strides in government statistical services that adheres to the ideals and vision of the government in serving the interest of society and the welfare of our nation.

SEC. 3. ***Definition of Terms.*** - As used in this Act, the following terms shall mean:

a. *Big Data*- datasets, whose volume is beyond the ability of typical database software tools to capture, store, manage and analyze within a tolerable elapsed period of time.

b. *Crowd source*- the process of soliciting information, ideas or feedback from a large group of people.

c. *Data Anonymity*- process of ensuring that personal information cannot be linked to a particular unique name of a citizen.

d. *Issue* - a fundamental problem with broad economic and scientific impact, whose solution will require the application of high-performance computing resources.

e. *Opt-In*- Permission given by the individual to volunteer particular personal data for Big Data analytics.

SEC. 4. ***Establishment of the Center.*** - There shall be established a Big Data Center that shall be attached to the Philippine Statistical Research and Training Institute (PSRTI). The National Big Data Center in the Philippines shall be hereinafter referred to as the "Big Data Center" (BDC).

SEC. 5. ***Powers and Functions.*** - The Big Data Center shall have the following powers and functions:

a. Develop a Big Data research program that will address emerging development issues;

b. Build partnerships with both public sector agencies and private sector agencies for the conduct of research that examines digital data sources for producing alternative statistics to meet information requirements for socio-economic development goals;

c. Provide government and development partners with valuable information generated from alternative near real-time data sources that shall complement statistics generated by the Philippine Statistics Authority (PSA) and other statistics producing agencies in the Philippine Statistical System;

d. Establish and administer capacity building activities on Big Data analytics for various partner institutions.

SEC. 6. ***Composition.*** - The Big Data Center shall be composed of the Office of the Director and the Offices of the following Divisions: *a) Open Data Division; b) Partnerships Division; c) Data Analytics and Storage Division;* and, *d) Privacy and Data Anonymity Division.*

SEC. 7. ***Office of the Director.*** – The Office of the Director shall consist of the Director and his or her immediate staff.

SEC. 8. ***Director.*** - The Director shall be appointed by the PSRTI Board of Directors.

The Director shall have the following powers and functions:

a. Ensure the development and regular updating of the Big Data Laboratory Research Program;
b. Implement the Big Data Program and monitor the progress of the research activities of the Center;
c. Convene quarterly the Technical Advisory Committee on Big Data, Open Data Division, Partnerships Division, Data Analytics and Storage Division and the Privacy and Data Anonymity Division as defined in this Act for an independent assessment of the research activities and the Big Data Program; and
d. Submit to the President of PSRTI an Annual Report on the accomplishments of the Center.

SEC. 9. ***Technical Advisory Committee on Big Data.*** - A Technical Advisory Committee (TAC) on Big Data shall be created in order to provide guidance to the Big Data Center and PSRTI on the program and activities of the Center. TAC members shall have a term of three (3) years and shall be composed of an appointive chair and four appointive members who are experts from the following disciplinary groups:

a. Social Science (anthropology, economics, political science, psychology and sociology);
b. Natural and Geological Science;
c. Statistics;
d. Computer Science; and
e. Information Technology

SEC. 10. ***Open Data Division.*** - An Open Data Division shall be created to perform the following functions:

a. Fully utilize and maximize existing Open Data from different government agencies for data analytics to aid in the development of the country;

b. Provide recommendations to different agencies on what other data shall be provided by the government in order to come up with a more comprehensive set of information available for data analytics;
c. Shall have the power to demand information deemed as Open Data from government agencies;
d. Ensure that the Big Data Center runs parallel with the Open Data initiative by amalgamating existing government information and providing data analytics towards the discovery of new and innovative solutions for government services;
e. Provide, publish and make available for download in universally accepted formats such as, but not limited to plain text, comma-separated values spreadsheet, or open standard multimedia data readily verifiable through a checksum standard as determined by the Internet Engineering Task Force or similar globally recognized standards organization; and
f. Work towards the transparency not just of information deemed public by Open Data standards but openness in the processes within the Big Data Center.

SEC. 11. ***Partnership Division.*** - A Partnership Division shall be created to perform the following functions:

a. Synergize with entities engaged in the operation and/or provision of information and communications, telecommunications and other multi-media infrastructures that include, but are not limited to, social media, Internet search engines, remote sensing and other available sources of data from existing information and communications technology tools;
b. Collaborate with data partners by coming up with an agreement that shall allow mobile companies, internet companies to share the data they have that can be used for the analysis in the Big Data Center;
c. Establish confidentiality, privacy, process of analytics and ownership of information in the Big Data holdings to partners; and
d. For the PSRTI and BDC to work out an agreement for research that will provide technical/statistical services to the partners in order to test new tools and eventually mainstream approaches for the application of the new digital data sources for the industries.

SEC. 12. ***Data Analytics and Storage Division.*** - A Data Analytics and Storage Division shall be created to perform the following functions.

a. Inspect, clean, transform and model data with the goal of discovering useful information, suggesting conclusions and supporting decision making;
b. Determine the appropriate data analysis technique that can help not just in purely descriptive purposes but also predictive purposes as may be deemed necessary;
c. Work towards efficiency in data storage utilizations by using less storage and space that can house the same amount of data and can ultimately reduce capital and operating costs; and
d. Provide for, but not limited to Operating Systems Security Specialists, Applications Security Specialists as well as Network Security Specialists to ensure the integrity of data and infrastructure.

SEC. 13. ***Privacy and Data Anonymity Division.*** – A Privacy and Data Anonymity Committee shall be created to ensure at all times the confidentiality of any personal information that comes to its knowledge and possession. The Committee shall ensure that the following standards on privacy shall be followed:

a. Ensure protection and security of any personal information that comes to its knowledge and possession;
b. Anonymize personal data even before going through the processing of data analytics. The data used and processed shall be in the form of anonymized data where the information gathered and processed may not be traced to a particular unique name of a citizen;
c. Establish opt-in permissions or a more secure permission system given the particular for stakeholders whose data shall be used;
d. Ensure that individuals or organizations are held accountable for protecting, securing and using personal data;
e. Bring to authorities offenses to the violations defined in this Act;
f. Ensure transparency and openness in the processes within the Big Data Center particularly in data analytics; and
g. Implement compliance measures for privacy standards as well as the adherence to the Data Privacy Act and other relevant privacy rules set by law.

The use and availability of accurate and complete information whenever it is required shall be limited to authorized users and shall be subject to the provisions of

Republic Act No. 10173, otherwise known as the Data Privacy Act of 2012, Commonwealth Act No. 591, otherwise known as An Act Creating the Bureau of Census and Statistic and further governed by Section 26 of RA 10625, otherwise known as the Philippine Statistical Act of 2013 and other applicable laws. Nothing in this Act shall be construed as to have amended or repealed Republic Act No. 1405, otherwise known as the Secrecy of Bank Deposits Act; Republic Act No. 6426, otherwise known as the Foreign Currency Deposit Act; and Republic Act No. 9510, otherwise known as the Credit Information System Act (CISA).

SEC. 14. ***Violations on Data Privacy.*** -

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

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

c. *Unauthorized authorization or granting of privileges.* – It shall be unlawful for any person to intentionally provide a third party authorization or privileges to access or modify data, networks, storage media where data is stored, equipment through which networks are run or maintained, the

physical plant where the data or network equipment is housed, without authority granted by the Internet service provider, telecommunications entity, or other such person providing Internet or data services having possession or control of the data or network, or to intentionally provide a third party authorization to access or modify intellectual property published on the Internet or on other networks without the consent of the person having ownership, possession, or control of the intellectual property, or without legal grounds, even if the authorization to access or perform modifications was granted without malice.

d. *Unauthorized disclosure.* – It shall be unlawful for any authorized person to intentionally disclose or cause the disclosure to a third party or to the public any private data being transmitted through the Internet or through public networks, or any data being transmitted through private networks, without legal grounds, even if the disclosure was done without malice.

e. *Violation of Data Privacy Act through ICT.* – It shall be unlawful to perform acts in violation of the Data Privacy Act of 2012 (RA 10175) using a device, network equipment, or physical plant connected to the Internet, public networks, private networks, or telecommunications facilities.

SEC. 15. ***Violation of Data Security.*** –

a. *Hacking.* – It shall be unlawful for any unauthorized person to intentionally access or to provide a third party with access to, or to hack or aid or abet a third party to hack into, data, networks, storage media where data is stored, equipment through which networks are run or maintained, the physical plant where the data or network equipment is housed. The unauthorized access or unauthorized act of providing a third party with access to, or the hacking into, data, networks, storage media where data is stored, equipment through which networks are run or maintained, the physical plant where the data or network equipment is housed shall be presumed to be malicious.

b. *Cracking.* – It shall be unlawful for any unauthorized person to intentionally modify or to crack data, networks, storage media where data is stored, equipment through which networks are run or maintained, the physical plant where the data or network equipment is housed, or for any unauthorized person to intentionally modify intellectual property published on the Internet or on other networks. The unauthorized

modification or cracking of data, networks, storage media where data is stored, equipment through which networks are run or maintained, the physical plant where the data or network equipment is housed, or unauthorized modification of intellectual property published on the Internet or on other networks, shall be presumed to be malicious.

c. *Phishing.* –

(i) It shall be unlawful for any unauthorized person to intentionally acquire or to cause the unauthorized acquisition, or identity or data theft, or phishing of private data, security information, or data or information used as proof of identity of another person. The unauthorized acquisition or causing to acquire, or identity or data theft, or phishing of private data, security information, or data or information used as proof of identity of another person shall be presumed to be malicious.

(ii) Malicious disclosure of unwarranted or false information relative to any personal information or personal sensitive information obtained by him or her as defined by Section 31 of the Data Privacy Act of 2012 (RA 10175) shall constitute phishing.

d. *Violation of Data Privacy Act in series or combination with hacking, cracking, or phishing.* – It shall be unlawful to perform acts in violation of the Data Privacy Act of 2012 (RA 10175) using a device, network equipment, or physical plant connected to the Internet, public networks, private networks, or telecommunications facilities performed in series or combination with acts prohibited by the preceding paragraphs.

SEC. 16. *Illegal and Arbitrary Seizure.* –

a. *Illegal Seizure.* – It shall be unlawful for any person to seize data, information, or contents of a device, storage medium, network equipment, or physical plant, or to seize any device, storage medium, network equipment, or physical plant connected to the Internet or to telecommunications networks of another person without his consent, or to gain possession or control of the intellectual property published on the Internet or on public networks of another person without his consent, except upon a final ruling from the courts, issued following due notice and hearing.

b. *Aiding and Abetting Illegal Seizure.* – It shall be unlawful for any person to aid or abet the seizure of data, information, or contents of a device,

storage medium, network equipment, or physical plant, or to seize any device, storage medium, network equipment, or physical plant connected to the Internet or to telecommunications networks of another person without his consent, or to gain possession or control of the intellectual property published on the Internet or on public networks of another person without his consent, except upon a final ruling from the courts, issued following due notice and hearing, allowing the person to perform such seizure, possession, or control.

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

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

SEC. 17. *Penalties.* -

a. Violation of Unauthorized access – shall be punishable with imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

b. Violation of Unauthorized modification - shall be punished with imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than

Two million pesos (Php2,000,000.00).

c. Violation of Unauthorized granting of privileges - shall be punished with imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

d. Violation of Unauthorized disclosure - imprisonment ranging from three (3) years to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

e. Violation of Data Privacy Act through ICT –

i. Violation of Section 25 (a) of the Data Privacy Act (Unauthorized Processing of Personal Information) through ICT – imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

ii. Violation of Section 25 (b) of the Data Privacy Act (Unauthorized Processing of Sensitive Personal Information) through ICT – imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

iii. Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal Information Due to Negligence) through ICT – imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

iv. Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive Personal Information Due to Negligence) through ICT – imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

v. Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of Personal Information) through ICT – imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00).

vi. Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of Sensitive Personal Information) through ICT – imprisonment ranging from one (1) year to three (3) years and a fine of

not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00).

vii. Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal Information for Unauthorized Purposes) through ICT – imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

viii. Violation of Section 28 (b) of the Data Privacy Act (Processing of Sensitive Personal Information for Unauthorized Purposes) through ICT – imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

ix. Violation of Section 30 of the Data Privacy Act (Concealment of Security Breaches Involving Sensitive Personal Information) through ICT – imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

Violation of Section 33 of the Data Privacy Act (Combination or Series of Acts) through ICT – imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

f. Violation of Hacking – imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

g. Violation of Cracking – imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

h. Violation of Phishing – imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

i. Violation of Data Privacy Act (with hacking, cracking, or phishing) –

i. Violation of Section 25 (a) of the Data Privacy Act (Unauthorized Processing of Personal Information) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging from one (1)

year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

ii. Violation of Section 25 (b) of the Data Privacy Act (Unauthorized Processing of Sensitive Personal Information) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

iii. Violation of Section 26 (a) of the Data Privacy Act (Accessing Personal Information Due to Negligence) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

iv. Violation of Section 26 (b) of the Data Privacy Act (Accessing Sensitive Personal Information Due to Negligence) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00).

v. Violation of Section 27 (a) of the Data Privacy Act (Improper Disposal of Personal Information) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging from six (6) months to two (2) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than Five hundred thousand pesos (Php500,000.00).

vi. Violation of Section 27 (b) of the Data Privacy Act (Improper Disposal of Sensitive Personal Information) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging from one (1) year to three (3) years and a fine of not less than One hundred thousand pesos (Php100,000.00) but not more than One million pesos (Php1,000,000.00).

vii. Violation of Section 28 (a) of the Data Privacy Act (Processing of Personal Information for Unauthorized Purposes) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging from one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not

more than One million pesos (Php1,000,000.00).

viii. Violation of Section 28 (b) of the Data Privacy Act (Processing of Sensitive Personal Information for Unauthorized Purposes) with hacking, cracking, or phishing – shall be penalized by imprisonment ranging from two (2) years to seven (7) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Two million pesos (Php2,000,000.00).

ix. Violation of Section 30 of the Data Privacy Act (Concealment of Security Breaches Involving Sensitive Personal Information) with hacking, cracking, or phishing – Shall be penalized by imprisonment of one (1) year and six (6) months to five (5) years and a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than One million pesos (Php1,000,000.00).

x. Violation of Section 33 of the Data Privacy Act (Combination or Series of Acts) with hacking, cracking, or phishing – Shall be penalized by imprisonment ranging from three (3) years to six (6) years and a fine of not less than One million pesos (Php1,000,000.00) but not more than Five million pesos (Php5,000,000.00).

j. Violation of Illegal seizure of ICT– shall be punished with imprisonment of *prison correccional* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

k. Violation of Aiding and abetting illegal seizure of ICT – shall be punished with imprisonment of *prison correccional* in its minimum period or a fine of not more than Four hundred thousand pesos (PhP400,000.00) or both.

l. Violation of Arbitrary seizure of ICT– Shall be punished with imprisonment of *prison correccional* in its maximum period or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

m. Violation of Instigating arbitrary seizure of ICT – shall be punished with imprisonment of *prison correccional* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

SEC. 18. ***Ownership of Data.***- Data that comes to the possession and knowledge of the Big Data Center shall be deemed as property of public dominion. Unprocessed data that comes to the possession of the Center shall be considered property of public dominion for public service where its use is limited to authorized persons in government. Processed data of the Center which shall take the form of official reports and studies shall

be deemed as property of public dominion for public use such that it is intended for the use of anybody. Data partners may define the ownership of data based on the partnership agreements with the government taking into consideration the context of the need of such data.

SEC. 19. ***Funding.*** -There shall be included in the budget of NEDA under the annual General Appropriations Act an amount of Two Hundred Million Pesos (P200,000,000.00) as the initial operating fund of the Big Data Center.

After the first year of implementation, such sums as may be necessary to fund the Big Data Center shall be included in the budget of NEDA under the annual General Appropriations Act.

Contributions, donations, bequests, grants and loans from domestic and/or foreign sources, government appropriations and other incomes accruing from the operations shall be allowed to be received and added to the funds and to be utilized exclusively by the Center.

SEC. 20. ***Implementing Rules and Regulations.*** – Within sixty (60) days from the effectivity of this Act, the Philippine Statistics Authority (PSA) shall promulgate the necessary rules and regulations for the effective implementation of this Act.

SEC. 21. ***Separability Clause.*** - Should any provision herein be declared unconstitutional, the same shall not affect the validity of the other provisions of this Act.

SEC. 22. ***Repealing Clause.*** - All laws, decrees, orders, rules, and regulations or other issuances or parts inconsistent with the provisions of this Act are hereby repealed or modified accordingly.

SEC. 23. ***Effectivity.*** - This Act shall take effect fifteen (15) days after its publication in the Official Gazette or in two (2) newspapers of general circulation in the Philippines.

Approved,