CONGRESS OF THE PHILIPPINES
FIFTEENTH CONGRESS
First Regular Session

HOUSE OF REPRESENTATIVES

H. No. 4115

BY REPRESENTATIVES ROMULO, YAP (S.), JALOSJOS (C.), TINGA, PALMONES, SARMIENTO (M.), KHO (D.), TREÑAS, VILLAFUERTE, APACIBLE AND HERRERA-DY, PER COMMITTEE REPORT NO. 554

AN ACT PROTECTING INDIVIDUAL PERSONAL DATA IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND IN THE PRIVATE SECTOR, PROVIDING PENALTIES IN VIOLATION THEREOF, AND FOR OTHER PURPOSES

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

CHAPTER I

GENERAL PROVISIONS

SECTION 1. *Short Title*. – This Act shall be known as the "Data Privacy Act of 2011".

SEC. 2. *Declaration of Policy*. – It is the policy of the State to protect the fundamental human right of privacy of communication. The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected.

SEC. 3. *Definition of Terms*. – Whenever used in this Act, the following terms shall have the respective meanings hereafter set forth:

(a) *Commission* refers to the Commission on Information and Communications Technology (CICT).

(b) *Consent of the data subject* refers to any freely given, specific and informed expression of will, either in written or electronic form executed personally and voluntarily by the data subject, whereby the data subject agrees to the processing of personal information about and/or relating to him or her.

(c) *Data subject* refers to an individual whose personal information is processed.

(d) *Direct marketing* refers to communication by whatever means of any advertising or marketing material which is directed to particular individuals.

(e) *Filing system* refers to any set of information relating to natural or juridical persons to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular person is readily accessible.

(f) *Information and communications system* refers to a system for 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, transmitted or stored and any procedure related to the recording, transmission or storage of electronic data message or electronic document.

(g) *Personal information* refers to any information, or any opinion, whether true or not and whether recorded in a material form or not, from which the identity of an individual is apparent to or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would identify an individual.

(h) *Personal information controller* refers to a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf. The term excludes:

(1) A person or organization who performs such functions as instructed by another person or organization; and

(2) An individual who collects, holds, processes or uses personal information in connection with the individual's personal, family or household affairs.

(i) *Personal information processor* refers to any natural or juridical person qualified to act as such under this Act to whom a personal information controller may outsource the processing of personal data pertaining to a data subject.

(j) *Privileged information* refers to any and all forms of data which under the Rules of Court and other pertinent laws constitute privileged communication.

(k) *Processing* refers to any operation or any set of operations performed upon personal information including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of data.

(l) *Sensitive personal information* refers to personal information:

(1) About an individual's race, ethnic origin, marital status, age, color and religious, philosophical or political affiliations;

(2) About an individual's health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;

(3) Issued by government agencies peculiar to an individual which includes, but not limited to, Social Security numbers, previous or current

health records, licenses or its denials, suspension or revocation, and tax returns; and

(4) Specifically established by an executive order or an act of Congress to be kept classified.

SEC. 4. *Scope.* – This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines subject to the immediately succeeding paragraph: *Provided, further,* That the requirements of Section 5 are complied with.

This Act does not apply to the following:

(a) Information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

(1) The fact that the individual is or was an officer or employee of the government institution;

(2) The title, business address and office telephone number of the individual;

(3) The classification, salary range and responsibilities of the position held by the individual; and

(4) The name of the individual on a document prepared by the individual in the course of employment with the government;

(b) Information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to

an individual, including the name of the individual and the exact nature of the benefit;

(d) Personal information processed for journalistic, artistic or literary purposes; and

(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent central monetary authority and law enforcement agencies of their constitutionally and statutorily mandated functions.

SEC. 5. *Extraterritorial Application*. – This Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

(a) The act, practice or processing relates to personal information about a Philippine citizen or a resident;

(b) The entity has a link with the Philippines, and the entity is processing personal information in the Philippines or even if the processing is outside the Philippines as long as it is about Philippine citizens or residents such as, but not limited to, the following:

(1) A contract is entered in the Philippines;

(2) A juridical entity unincorporated in the Philippines but has central management and control in the country; and

(3) An entity that has a branch, agency, office or subsidiary in the Philippines and the parent or affiliate of the Philippine entity has access to personal information; and

(c) The entity has other links in the Philippines such as, but not limited to:

(1) The entity carries on business in the Philippines; and

(2) The personal information was collected or held by an entity in the Philippines.

CHAPTER II

ADMINISTRATION AND IMPLEMENTATION

SEC. 6. *Implementing Agency*. – In addition to its existing functions, the Commission on Information and Communications Technology, hereinafter

referred to as the Commission, is hereby tasked to administer and implement the provisions of this Act, and to monitor and ensure compliance of the country with international standards set for data protection. The Commission shall perform the following functions:

(a) Ensure compliance of personal information controllers with the provisions of this Act;

(b) Receive complaints, institute investigations, facilitate or enable settlement of complaints through the use of alternative dispute resolution processes, adjudicate, award indemnity on matters affecting any personal information, prepare reports on disposition of complaints and resolution of any investigation it initiates, and, in cases it deems appropriate, publicize any such report: *Provided,* That in resolving any complaint or investigation (except where amicable settlement is reached by the parties), the Commission shall act as a collegial body. For this purpose, the Commission may be given access to personal information that is subject of any complaint and to collect the information necessary to perform its functions under this Act;

(c) Issue cease and desist orders, impose a temporary or permanent ban on the processing of personal information, upon finding that the processing will be detrimental to national security and public interest;

(d) Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy;

(e) Monitor the compliance of other government agencies or instrumentalities on their security and technical measures, and recommend the necessary action in order to meet minimum standards for protection of personal information pursuant to this Act;

(f) Coordinate with other government agencies and the private sector on efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country;

(g) Publish on a regular basis a guide to all laws relating to data protection;

(h) Publish a compilation of agency system of records and notices, including index and other finding aids;

(i) Recommend to the Department of Justice the prosecution and imposition of penalties of criminal offenses specified in this Act;

(j) Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers as well as other private sector self-regulatory initiatives: *Provided,* That the privacy codes or self-regulatory initiatives shall adhere to, and provide effective means of enforcing, the underlying data privacy principles embodied in this Act: *Provided, further,* That such privacy codes or self-regulatory initiatives may include private dispute resolution mechanisms for complaints against any participating personal information controller;

(k) Provide assistance on matters relating to privacy or data protection at the request of a national or local agency, a private entity or any person;

(1) Comment on the implication on data privacy of proposed national or local statutes, regulations or procedures, issue advisory opinions and interpret the provisions of this Act and other data privacy laws;

(m) Propose legislation, amendments or modifications to Philippine laws on privacy or data protection as may be necessary;

(n) Ensure proper and effective coordination with data privacy regulators in other countries and private accountability agents, participate in international and regional initiatives for data privacy protection, and generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection;

(o) Negotiate and contract with other data privacy authorities of other countries for cross-border application and implementation of respective privacy laws;

(p) Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations; and

(q) Report annually to Congress and to the President of the Republic of the Philippines on the activities of the Commission in carrying out the provisions of this Act.

SEC. 7. *Confidentiality.* – The Commission shall ensure at all times the confidentiality of any personal information that comes to its knowledge and possession.

SEC. 8. *Immunity*. – No criminal or civil proceedings shall lie against the Chairman of the Commission and its Commissioners, or any person acting on their behalf or under their direction, for anything done, reported or said in good faith as a result of the performance or exercise or purported performance or exercise, of any duty or power under this Act.

CHAPTER III

PROCESSING OF PERSONAL INFORMATION

SEC. 9. *General Data Privacy Principles.* – The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of transparency, legitimate purpose and proportionality.

Personal information must be:

(a) Collected for specified and legitimate purposes determined and declared before, or as soon as reasonably practicable, and later processed in a way compatible with such declared, specified and legitimate purposes only;

(b) Processed fairly and lawfully;

(c) Accurate, relevant and, where necessary for the processing of personal information, kept up to date; inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted;

(d) Adequate and not excessive in relation to the purposes for which they are collected and processed;

(e) Retained only for as long as necessary for the fulfillment of the purposes for which the data was obtained or as provided by law; and

(f) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed: *Provided,* That personal information collected for other purposes may be processed for historical, statistical or scientific purposes, and in cases laid down in law may be stored for longer periods: *Provided, further,* That adequate safeguards are guaranteed by said laws authorizing their processing.

The personal information controller must ensure implementation of personal information processing principles set out herein.

SEC. 10. *Criteria for Lawful Processing of Personal Information.* – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exist:

(a) The data subject has given his or her unambiguous consent, specific to the purpose which must be given in writing, or through any other similar means of express consent according to the circumstances;

(b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;

(c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

(d) The processing is necessary to protect vitally important interests of the data subject, including life and health; or

(e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

SEC. 11. *Sensitive Personal Information and Privileged Information.* – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:

(a) The data subject has given his or her consent, specific to the purpose prior to the processing, or in the case of privileged information, all parties to the exchange have given their consent prior to processing;

(b) The processing of the same is provided for by existing laws and regulations: *Provided,* That such regulatory enactments guarantee the protection of the sensitive personal information and the privileged information: *Provided, further,* That the consent of the data subjects are not required by law or regulation permitting the processing of the sensitive personal information or the privileged information;

(c) The processing is necessary to protect the life and health of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

(d) The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations: *Provided,* That such processing is only confined and related to the *bona fide* members of these organizations or their associations: *Provided, further,* That the sensitive personal information are not transferred to third parties: *Provided, finally,* That consent of the data subject was obtained prior to processing;

(e) The processing is necessary for purposes of medical treatment, is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal information is ensured; or

(f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings.

SEC. 12. *Subcontract of Personal Information.* – A personal information controller may subcontract the processing of personal information: *Provided,* That the personal information controller shall be responsible for ensuring that proper safeguards are in place to ensure the confidentiality of the personal information processed, prevent its use for unauthorized purposes, and generally, comply with the requirements of this Act and other laws for processing of personal information. The personal information processor shall comply with all the requirements of this Act and other applicable laws.

SEC. 13. *Storage of Data.* – Personal information shall be stored and used only for as long as it is necessary to achieve the purpose for which it was processed, after which the personal information shall be deleted or blocked from a personal information base, unless otherwise provided by law.

SEC. 14. *Extension of Privileged Communication.* – Personal information controllers may invoke the principle of privileged communication over privileged information that they lawfully control or process. Subject to existing laws and regulations, any evidence gathered on privileged information is inadmissible.

CHAPTER IV

RIGHTS OF THE DATA SUBJECT

SEC. 15. *Rights of the Data Subject.* – The data subject is entitled to:

(a) Be informed whether personal information pertaining to him or her shall be, are being or have been processed;

(b) Be furnished the information indicated hereunder before the entry of his or her personal information into the processing system of the personal information controller, or at the next practical opportunity:

(1) Description of the personal information to be entered into the system;

(2) Purposes for which they are being or are to be processed;

(3) Scope and method of the personal information processing;

(4) The recipients or classes of recipients to whom they are or may be disclosed; and

(5) Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized.

Any information supplied or declaration made to the data subject on these matters shall not be amended without prior notification of data subject: *Provided,* That the notification under subsection (b) shall not apply should the personal information be needed pursuant to a subpoena or when the collection and processing are for obvious purposes;

(c) Reasonable access to, upon demand, the following:

(1) Contents of his or her personal information that were processed;

(2) Sources from which personal information were obtained;

(3) Names and addresses of recipients of the personal information;

(4) Manner by which such data were processed;

(5) Reasons for the disclosure of the personal information to recipients;

(6) Information on automated processes where the data will or are likely to be made as the sole basis for any decision significantly affecting or will affect the data subject;

(7) Date when his or her personal information concerning the data subject were last accessed and modified; and

(8) The designation, or name, or identity and address of the personal information controller;

(d) Dispute the inaccuracy or error in the personal information and have the personal information controller correct it immediately and accordingly, unless the request is vexatious or otherwise unreasonable. If the personal information have been corrected, the personal information controller shall ensure the accessibility of both the new and the retracted information and the simultaneous receipt of the new and the retracted information by recipients thereof: *Provided,* That third parties who have previously received such processed personal information shall be informed of its inaccuracy and its rectification upon reasonable request of the data subject;

(e) Suspend, withdraw or order the blocking, removal or destruction of his or her personal information from the personal information controller's filing system upon discovery and substantial proof that the personal information are incomplete, outdated, false, unlawfully obtained, used for unauthorized purposes, used for direct marketing purposes, unless expressly authorized, or are no longer necessary for the purposes for which they were collected. In this case, the personal information controller may notify third parties who have previously received such processed personal information; and

(f) Be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal information.

SEC. 16. *Transmissibility of Rights of the Data Subject.* – The lawful heirs and assigns of the data subject may invoke the rights of the data subject for which he or she is an heir or assignee at any time after the death of the data subject or when the data subject is incapacitated or incapable of exercising the rights as enumerated in the immediately preceding section.

SEC. 17. *Non-applicability.* – The immediately preceding sections are not applicable if the processed personal information are used only for the needs of scientific and statistical research and, on the basis of such, no activities are carried out and no decisions are taken regarding the data subject: *Provided,* That the personal information shall be held under strict confidentiality and shall be used only for the declared purpose. Likewise, the immediately preceding sections are not applicable to processing of personal information gathered for the purpose of investigations in relation to any criminal, administrative or tax liabilities of a data subject.

CHAPTER V

SECURITY OF PERSONAL INFORMATION

SEC. 18. *Security of Personal Information.* – (a) The personal information controller must implement reasonable and appropriate organizational, physical and technical measures intended for the protection of personal information against any accidental or unlawful destruction, alteration and disclosure, as well as against any other unlawful processing.

(b) The personal information controller shall implement reasonable and appropriate measures to protect personal information against natural dangers such as accidental loss or destruction, and human dangers such as unlawful access, fraudulent misuse, unlawful destruction, alteration and contamination.

(c) The determination of the appropriate level of security under this section must take into account the nature of the personal information to be protected, the risks represented by the processing, the size of the organization

and complexity of its operations, current data privacy best practices and the cost of security implementation. Subject to guidelines as the Commission may issue from time to time, the measures implemented must include:

(1) Safeguards to protect its computer network against accidental, unlawful or unauthorized usage or interference with or hindering of their functioning or availability;

(2) A security policy with respect to the processing of personal information;

(3) A process for identifying and assessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action for such vulnerabilities; and

(4) Regular monitoring for security breaches and a process for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach.

(d) The personal information controller must further ensure that third parties processing personal information on its behalf shall implement the security measures required by this provision.

(e) The employees, agents or representatives of a personal information controller who are involved in the processing of personal information shall operate and hold personal information under strict confidentiality if these personal information are not intended for public disclosure. This obligation shall continue even after leaving the public service, transfer to another position or upon termination of employment or contractual relations.

(f) The personal information controller shall promptly notify the Commission and affected data subjects when sensitive personal information or other information that may, under the circumstances, be used to enable identity fraud are reasonably believed to have been acquired by an unauthorized person, and the personal information controller or the Commission believes that such unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject. The notification shall at least describe the nature of the breach, the sensitive personal information possibly involved, and

the measures taken by the entity to address the breach. Notification may be delayed only to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system.

(1) In evaluating if notification is warranted, the Commission may take into account compliance by the personal information controller with this section and existence of good faith in the acquisition of personal information.

(2) The Commission may exempt a personal information controller from notification where, in its reasonable judgment, such notification would not be in the public interest or in the interests of the affected data subjects.

(3) The Commission may authorize postponement of notification where it may hinder the progress of a criminal investigation related to a serious breach.

CHAPTER VI

ACCOUNTABILITY FOR TRANSFER OF PERSONAL INFORMATION

SEC. 19. *Principle of Accountability*. – Each personal information controller is responsible for personal information under its control or custody, including information that have been transferred to a third party for processing, whether domestically or internationally, subject to cross-border arrangement and cooperation.

(a) The personal information controller is accountable for complying with the requirements of this Act and shall use contractual or other reasonable means to provide a comparable level of protection while the information are being processed by a third party.

(b) The personal information controller shall designate an individual or individuals who are accountable for the organization's compliance with this Act. The identity of the individual(s) so designated shall be made known to any data subject upon request.

CHAPTER VII

SECURITY OF SENSITIVE PERSONAL INFORMATION IN GOVERNMENT

SEC. 20. *Responsibility of Heads of Agencies.* – All sensitive personal information maintained by the government, its agencies and instrumentalities shall be secured, as far as practicable, with the use of the most appropriate standard recognized by the information and communications technology industry, and as recommended by the Commission. The head of each government agency or instrumentality shall be responsible for complying with the security requirements mentioned herein while the Commission shall monitor the compliance and may recommend the necessary action in order to satisfy the minimum standards.

SEC. 21. *Requirements Relating to Access by Agency Personnel to Sensitive Personal Information.* –

(a) On-site and Online Access – Except as may be allowed through guidelines to be issued by the Commission, no employee of the government shall have access to sensitive personal information on government property or through online facilities unless the employee has received a security clearance from the head of the source agency.

(b) Off-site Access – Unless otherwise provided in guidelines to be issued by the Commission, sensitive personal information maintained by an agency may not be transported or accessed from a location off government property unless a request for such transportation or access is submitted and approved by the head of the agency in accordance with the following guidelines:

(1) Deadline for Approval or Disapproval – In the case of any request submitted to the head of an agency, such head of the agency shall approve or disapprove the request within two (2) business days after the date of submission of the request. In case there is no action by the head of the agency, then such request is considered disapproved;

(2) Limitation to One thousand (1,000) Records – If a request is approved, the head of the agency shall limit the access to not more than one thousand (1,000) records at a time; and

(3) Encryption – Any technology used to store, transport or access sensitive personal information for purposes of off-site access approved under this subsection shall be secured by the use of the most secure encryption standard recognized by the Commission.

The requirements of this subsection shall be implemented not later than six (6) months after the date of the enactment of this Act.

SEC. 22. *Applicability to Government Contractors.* – In entering into any contract that may involve accessing or requiring sensitive personal information from one thousand (l,000) or more individuals, an agency shall require a contractor and its employees to register their personal information processing system with the Commission in accordance with this Act and to comply with the other provisions of this Act including the immediately preceding section, in the same manner as agencies and government employees comply with such requirements.

CHAPTER VIII

PENALTIES

SEC. 23. *Offenses Involving Personal Information.* – The Commission shall impose a fine of not less than Two hundred thousand pesos (Php200,000.00) but not more than Two million pesos (Php2,000,000.00) for each violation of Sections 10 and 15 of this Act, with respect to personal information.

SEC. 24. *Offenses Involving Sensitive Personal Information*. – The Commission shall impose a fine of not less than Five hundred thousand pesos (Php500,000.00) but not more than Four million pesos (Php4,000,000.00) for each violation of Sections 9 and 14 of this Act, with respect to sensitive personal information.

SEC. 25. *Other Offenses.* – The Commission shall impose a fine of Two hundred thousand pesos (Php200,000.00) to Five million pesos (Php5,000,000.00) for the following offenses:

(a) Failure to issue a breach notification when warranted under Section 18(f);

(b) Failure to implement appropriate security measures under Section 18; and

(c) Other violations of this Act.

SEC. 26. *Commensurate to Harm.* – The fines to be issued by the Commission under Sections 23, 24 and 25 of this Act shall be commensurate to the severity of the harm caused, or likely to be caused by the offense under the circumstances.

SEC. 27. *Criminal Act.* – Offenses involving personal information and sensitive personal information under Sections 23 and 24 of this Act, when determined by the Department of Justice to be intentional in its separate and independent investigation, shall further be punishable by imprisonment ranging from one (1) year to three (3) years.

CHAPTER IX

MISCELLANEOUS PROVISIONS

SEC. 28. *Interpretation*. – Any doubt in the interpretation of any provision of this Act shall be liberally interpreted in favor of the rights and interests of the individual whose personal information are processed.

SEC. 29. *Implementing Rules and Regulations.* – Within ninety (90) days from the effectivity of this Act, the Commission shall promulgate the rules and regulations to effectively implement the provisions of this Act.

SEC. 30. *Reports and Information.* – The Commission shall annually report to the President and Congress on its activities in carrying out the provisions of this Act. The Commission shall undertake whatever efforts it may determine to be necessary or appropriate to inform and educate the public of data privacy, data protection and fair information rights and responsibilities.

SEC. 31. *Transitory Provision*. – In case the Commission is abolished, the administration and implementation of this Act shall be transferred to the National Telecommunications Commission (NTC).

SEC. 32. *Separability Clause.* – If any part or provision of this Act shall be held unconstitutional or invalid, the other provisions hereof that are not affected thereby shall continue to be in full force and effect.

SEC. 33. *Repealing Clause.* – The provision of Section 7 of Republic Act No. 9372, otherwise known as the "Human Security Act of 2007", is hereby amended. All other laws, decrees, executive orders, proclamations and administrative regulations or parts thereof inconsistent herewith are hereby repealed or modified accordingly.

SEC. 34. *Effectivity Clause.* – This Act shall take effect fifteen (15) days after its publication in at least two (2) national newspapers of general circulation.

Approved,

O