

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

28 September 2016

OHCHR REGISTRY

DAVID KAYE
Special Rapporteur
Office of the UN High Commissioner for Human Rights
Palais des Nations, Geneva, Switzerland

14 OCT 2016

Recipients: SPB
.....
.....
.....

Dear Mr. Kaye:

This pertains to your letter dated 9 August 2016 requesting for information on the relevant national legal frameworks regarding freedom of expression and the telecommunications and internet access sector.

With regard to laws permitting authorities to require telecommunications and Internet Service Providers (ISPs) to suspend or restrict access to websites or internet and telecommunications networks or provide and facilitate access to customer data, please be informed that:

Under the Anti-Wiretapping Law, a law enforcer may be authorized by court to intercept or wiretap in cases involving the crimes of treason, espionage, proving war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping and violations of Commonwealth Act No. 616.

Under the Cybercrime Prevention Act, disclosure of computer data and search, seizure, and examination of computer data may be allowed through court-issued warrant.

With regard to laws requiring public disclosure of requests made or actions taken to suspend or restrict access to websites and telecommunications networks, and the requests to provide or facilitate access to customer data, please be informed that:

Under EO No. 2, citizens have access to information from certain government agencies, especially those under the Executive.

Under the Data Privacy Act, a set of criteria is established before personal information and sensitive personal information may be processed. A salient requirement before the processing of personal information and sensitive personal information is consent. The Data Privacy Act also requires that an individual be notified before the processing of his personal information.

With regard to laws, regulations, and other measures that govern the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers, and internet exchange points, please be informed that:

REPUBLIC OF THE PHILIPPINES

**DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY**

Under Public Telecommunications Policy Act, telecommunications entities, in particular, local exchange operators, inter-exchange operators, international carriers, and value-added service providers, mobile radio services, and radio paging services, are regulated and are required to conform to certain statutory requirements identified in the Act.

With regard to remedies available in the event of undue restriction on internet and telecommunications access or undue access to customer data:

Under the Cybercrime Prevention Act, illegal access, illegal interception, data interference, system interference, and computer related fraud are criminal offenses.

Under the Writ of Habeas Data , a person may file a case against an individual who threatens the petitioner's right to privacy by the respondent's acts or omissions.

Under the Data Privacy Act, a data subject is entitled to be informed when personal information pertaining to the data subject shall be, is being, or will be processed, and to be furnished with certain details regarding the information to be processed. The data subject may also dispute errors; suspend, withdraw or block personal information in certain cases; and be indemnified for damages.

Under the Data Privacy Act, personal information controllers are also required to 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.

With regard to other relevant laws that promote or enhance internet accessibility and connectivity, including measures to promote network neutrality:

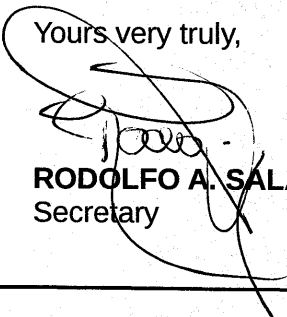
Under the Public Telecommunications Policy Act, end users have the right to utility service which is non-discriminatory, reliable, and which conforms to the minimum standards set by the National Telecommunications Commission. The said law also provides for the equality of treatment in the telecommunications industry.

Under the Electronic Commerce Act, lawful access electronic files shall be given only to those who have a right.

Excerpts of the specific, relevant sections in the aforementioned laws are attached to this letter. We hope that our input is of help in your endeavors. For any questions, comments, or for any other matters in which we can extend our assistance, please feel free to contact us.

Warm regards and best wishes.

Yours very truly,


RODOLFO A. SALALIMA
Secretary

DICT Building, C.P. Garcia Avenue,
Diliman, Quezon City 1101 Trunkline (+632) 920-0101

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

Excerpt of Relevant Laws

Relevant laws are identified as follows:

1. RA No. 4200 - Anti-Wiretapping Law
2. RA No. 7925 - Public Telecommunications Policy Act
3. RA No. 8792 - Electronic Commerce Act
4. RA No. 10173 - Data Privacy Act
5. RA No. 10175 - Cybercrime Prevention Act
6. EO No. 2, series of 2016 – Operationalizing Freedom of Information
7. A.M. No. 8-01-16-SC – The Rule on the Writ of Habeas Data

Excerpts to specific questions solicited in Mr. David Kaye's, Special Rapporteur, letter are as follows:

Item 1

Laws permitting authorities or requiring telecommunications and Internet Service Providers (ISPs) to suspend or restrict access to websites or internet and telecommunications networks or provide and facilitate access to customer data.

Summary:

Under the Anti-Wiretapping Law, a law enforcer may be authorized by court to intercept or wiretap in cases involving the crimes of treason, espionage, proving war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping and violations of Commonwealth Act No. 616.

Under the Cybercrime Prevention Act, disclosure of computer data and search, seizure, and examination of computer data may be allowed through court-issued warrant.

Relevant excerpts:

RA No. 4200, "Anti-Wiretapping Law"

Section 3. Nothing contained in this Act, however, shall render it unlawful or punishable for any peace officer, who is authorized by a written order of the Court, to execute any of the acts declared to be unlawful in the two preceding sections in cases involving the crimes of treason, espionage, provoking war and disloyalty in case of war, piracy, mutiny in the high seas, rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, inciting to sedition, kidnapping as defined by the Revised Penal Code, and violations of Commonwealth Act No. 616, punishing espionage and other offenses against national security: *Provided*, That such written order shall only be issued or granted upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and a showing: (1) that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed or is being committed or is about to be committed:

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

Provided, however, That in cases involving the offenses of rebellion, conspiracy and proposal to commit rebellion, inciting to rebellion, sedition, conspiracy to commit sedition, and inciting to sedition, such authority shall be granted only upon prior proof that a rebellion or acts of sedition, as the case may be, have actually been or are being committed; (2) that there are reasonable grounds to believe that evidence will be obtained essential to the conviction of any person for, or to the solution of, or to the prevention of, any of such crimes; and (3) that there are no other means readily available for obtaining such evidence.

The order granted or issued shall specify: (1) the identity of the person or persons whose communications, conversations, discussions, or spoken words are to be overheard, intercepted, or recorded and, in the case of telegraphic or telephonic communications, the telegraph line or the telephone number involved and its location; (2) the identity of the peace officer authorized to overhear, intercept, or record the communications, conversations, discussions, or spoken words; (3) the offense or offenses committed or sought to be prevented; and (4) the period of the authorization. The authorization shall be effective for the period specified in the order which shall not exceed sixty (60) days from the date of issuance of the order, unless extended or renewed by the court upon being satisfied that such extension or renewal is in the public interest.

RA 10175, "Cybercrime Prevention Act"

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

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

- (a) To secure a computer system or a computer data storage medium;
- (b) To make and retain a copy of those computer data secured;
- (c) To maintain the integrity of the relevant stored computer data;
- (d) To conduct forensic analysis or examination of the computer data storage medium; and
- (e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, 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.

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

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.

Item 2

Laws requiring public disclosure of requests made or actions taken to suspend or restrict access to websites and telecommunications networks, and the requests to provide or facilitate access to customer data.

Summary:

Under EO No. 2, citizens have access to information from certain government agencies, especially those under the Executive.

Under the Data Privacy Act, a set of criteria is established before personal information and sensitive personal information may be processed. A salient requirement before the processing of personal information and sensitive personal information is consent. The Data Privacy Act also requires that an individual be notified before the processing of his personal information.

Relevant excerpts:

Executive Order No. 2, Series of 2016

SECTION 3. Access to information. Every Filipino shall have access to information, official records, public records and to documents and papers pertaining to official acts, transactions or decisions, as well as to government research data used as basis for policy development.

SECTION 4. Exception. Access to information shall be denied when the information falls under any of the exceptions enshrined in the Constitution, existing law or jurisprudence.

The Department of Justice and the Office of the Solicitor General are hereby directed to prepare an inventory of such exceptions and submit the same to the Office of the President within thirty (30) calendar days from the date of effectivity of this Order.

The Office of the President shall thereafter, immediately circularize the inventory of exceptions for the guidance of all government offices and instrumentalities covered by this Order and the general public.

Said inventory of exceptions shall periodically be updated to properly reflect any change in existing law and jurisprudence and the Department of Justice and the Office of the Solicitor General are directed to update the inventory of exceptions as the need to do so arises, for circularization as hereinabove stated.

**DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY**

RA 10173, "Data Privacy Act"

Section 12. *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 exists:

- (a) The data subject has given his or her consent;

Section 13. *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;

Section 16. *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;

Section 4. Scope.

xxx

This Act does not apply to the following:

- (a) Information about any 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 service 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;

**DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY**

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

(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 and regulatory agencies of their constitutionally and statutorily mandated functions. 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);

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

Item 3

Laws, regulations, and other measures that govern the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers, and internet exchange points.

Summary:

RA 7925 regulates Article IV regulates telecommunications entities, in particular, local exchange operators, inter-exchange operators, international carriers, and value-added service providers, mobile radio services, and radio paging services.

Relevant excerpts:

RA 7925, "Public Telecommunications Policy Act of the Philippines"

Section 8. *Local Exchange Operator.* - A local exchange operator shall:

(a) provide universal basic telephone service to all subscribers who applied for such service, within a reasonable period and at such standards as may be prescribed by the Commission and at such tariff as to sufficiently give it a fair return on its investments.

(b) be protected from uncompensated bypass or overlapping operations of other telecommunications entities in need of physical links or connections to

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

its customers in the area except when it is unable to provide, within a reasonable period of time and at desired standard, the interconnection arrangements required by such entities.

(c) have the first option to provide pay telephone services or public calling stations in the area covered by its network.

(d) be entitled to a fair and equitable revenue sharing arrangement with the inter-exchange carrier or such other carriers connected to its basic network.

Section 9. *Inter-Exchange Carrier*. - The number of entities allowed to provide inter-exchange national long distance services may be limited, but as a matter of policy, where it is economically viable, at least two (2) carriers, shall be authorized: Provided, however, That a local exchange carrier shall not be restricted from operating its own inter-exchange carrier service if its viability is dependent thereto. Such inter-exchange carrier shall have the following obligations:

(a) It shall interconnect with other networks in the same category and with local exchange carriers or other telecommunications entities, upon application and within a reasonable time period, and under fair and reasonable level charges, in order that domestic and international long distance services are made possible; and

(b) It shall have the right to establish and operate its own tandem switching facilities to which international calls or overseas carriers have to course their messages or signals.

Section 10. *International Carrier*. - Only entities which will provide local exchange services and can demonstrably show technical and financial capability to install and operate an international gateway facility shall be allowed to operate as an international carrier.

The entity so allowed shall be required to produce a firm correspondent or interconnection relationships with major overseas telecommunications authorities or carriers within one (1) year from the grant of the authority.

The international carrier shall also comply with its obligations to provide the local exchange service in unserved or underserved areas within three (3) years from the grant of the authority as required by existing regulations: Provided, however, That said carrier shall be deemed to have complied with the said obligation in the event it allows an affiliate thereof to assume such obligation and who complies therewith.

Failure to comply with the above obligations shall be a cause to cancel its authority or permit to operate as an international carrier.

Section 11. *Value-added Service Provider*. - Provided that it does not put up its own network, a VAS provider need not secure a franchise. A VAS provider shall be allowed to competitively offer its services and/or expertise, and lease or rent telecommunications equipment and facilities necessary to provide such specialized services, in the domestic and/or international market in accordance with network compatibility.

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

Telecommunications entities may provide VAS, subject to the additional requirements that:

- (a) prior approval of the Commission is secured to ensure that such VAS offerings are not cross-subsidized from the proceeds of their utility operations;
- (b) other providers of VAS are not discriminated against in rates nor denied equitable access to their facilities; and
- (c) separate books of accounts are maintained for the VAS.

Section 12. *Mobile Radio Services.* - In a local telephone exchange area, more than one duly enfranchised provider of mobile radio services, distinct and separate from the local exchange carrier, may be allowed to operate. However, such entities shall secure prior authority from the Commission and, in addition, comply with the conditions imposed on VAS and with the norms on radio frequency spectrum utilization.

The operator of a mobile radio telephone system shall comply with its obligations to provide local exchange service in unserved and underserved areas in accordance with existing regulations. Failure to comply with this obligation within (3) years from the grant of the authority shall be a cause to cancel its authority or permit to operate a mobile radio telephone system.

Section 13. *Radio Paging Services.* - Duly enfranchised radio paging services involving either voice or data messages, shall be allowed to compete freely in rates, number of operators, or variety of operating modalities, subject only to the norms on radio frequency spectrum utilization.

Item 4

Remedies available in the event of undue restriction on internet and telecommunications access or undue access to customer data.

Summary:

Under the Cybercrime Prevention Act, illegal access, illegal interception, data interference, system interference, and computer related fraud are criminal offenses.

Under the Writ of Habeas Data , a person may file a case against an individual who threatens the petitioner's right to privacy by the respondent's acts or omissions.

Under the Data Privacy Act, a data subject is entitled to be informed when personal information pertaining to the data subject shall be, is being, or will be processed, and to be furnished with certain details regarding the information to be processed. The data subject may also dispute errors; suspend, withdraw or block personal information in certain cases; and be indemnified for damages.

Under the Data Privacy Act, personal information controllers are also required to implement reasonable and appropriate organizational, physical and technical

**DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY**

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.

Relevant excerpts:

A.M. No. 8-01-16-SC, "The Rule on the Writ of Habeas Data"

Section 1. Habeas Data. - The writ of habeas data is a remedy available to any person whose right to privacy in life, liberty or security is violated or threatened by an unlawful act or omission of a public official or employee, or of a private individual or entity engaged in the gathering, collecting or storing of data or information regarding the person, family, home and correspondence of the aggrieved party.

RA 10175, "Cybercrime Prevention Act"

Sec. 4 Cybercrime Offenses.

(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 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.

(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.

(1) **Computer-related Forgery.** —

(i) 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

(ii) 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

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

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.

RA 10173, “Data Privacy Act”

Section 16. *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;

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

(6) The identity and contact details of the personal information controller or its representative;

(7) The period for which the information will be stored; and

(8) The existence of their rights, i.e., to access, correction, as well as the right to lodge a complaint before the Commission.

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, including when it is necessary for the performance of or in relation to a contract or service or when necessary or desirable in the context of an employer-employee relationship, between the collector and the data subject, or when the information is being collected and processed as a result of legal obligation;

**DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY**

(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 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 the 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 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.

**DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY**

Section 20. *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 accessing reasonably foreseeable vulnerabilities in its computer networks, and for taking preventive, corrective and mitigating action against security incidents that can lead to a security breach; 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 the 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.

**DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY**

(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 (but 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 unwarranted, 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.

Item 5

Other relevant laws that promote or enhance internet accessibility and connectivity, including measures to promote network neutrality.

Summary:

Under the Public Telecommunications Policy Act, end users have the right to utility service which is non-discriminatory, reliable, and which conforms to the minimum standards set by the National Telecommunications Commission. The said law also provides for the equality of treatment in the telecommunications industry.

Under the Electronic Commerce Act, lawful access electronic files shall be given only to those who have a right.

Relevant excerpts:

RA 7925, "Public Telecommunications Policy Act"

Section 20. *Rights of End-Users.* - The user of telecommunications service shall have the following basic rights:

REPUBLIC OF THE PHILIPPINES

DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY

- (a) Entitlement of utility service which is non-discriminatory, reliable and conforming with minimum standards set by the Commission;
- (b) Right to be given the first single-line telephone connection or the first party-line connection within two (2) months of application for service, against deposit; or within three (3) months after targeted commencement of service in the barangay concerned per the original schedule of service expansion approved by the Commission, whichever deadline comes later;
- (c) Regular, timely and accurate billing, courteous and efficient service at utility business offices and by utility company personnel; and
- (d) Thorough and prompt investigation of, and action upon complaints. The utility shall endeavor to allow complaints to be received over the telephone and shall keep a record of all written or phoned-in complaints.

Section 23. *Equality of Treatment in the Telecommunications Industry.* - Any advantage, favor, privilege, exemption, or immunity granted under existing franchises, or may hereafter be granted, shall ipso facto become part of previously granted telecommunications franchises and shall be accorded immediately and unconditionally to the grantees of such franchises: Provided, however, That the foregoing shall neither apply to nor affect provisions of telecommunications franchises concerning territory covered by the franchise, the life span of the franchise, or the type of service authorized by the franchise.

RA 8792, "Electronic Commerce Act"

Section 31. *Lawful Access.* - Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of plaintext, electronic signature or file or solely for the authorized purposes. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key;



DEPARTMENT OF FOREIGN AFFAIRS
KAGAWARAN NG UGNAYANG PANLABAS

19013

OFFICE OF UNITED NATIONS
AND INTERNATIONAL ORGANIZATIONS

URGENT

31 August 2016

Sir:

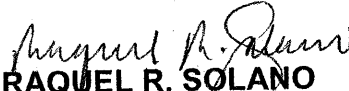
The Department of Foreign Affairs wishes to refer to your office a Note Verbale from the UN Office of the High Commissioner for Human Rights (OHCHR) transmitting a letter from Mr David Kaye, Special Rapporteur on the "Right to Freedom of Opinion and Expression," requesting for inputs on a thematic report that will be presented during the 35th session of the Human Rights Council in June 2017.

The report will focus on freedom of expression in the telecommunications and Internet access sector. It will examine State regulation and action that affect access to telecommunications and Internet networks and services, particularly those provided by Telecommunications and Internet Service Providers. It will also analyze relevant internal practices, policies, and practices of telecommunication companies, internet service providers, and associated businesses.

In this regard, the DFA requests DICT's comments and inputs on the attached questionnaire from the Special Rapporteur. For further details, Messrs. Paolo Zurita or David Bien Paje of this office may be reached through unio.div6@gmail.com and telephone number 834 4913.

With my best regards.

Very truly yours,
For the Assistant Secretary:


RAQUEL R. SOLANO
Executive Director

MR. RODOLFO A. SALALIMA

Secretary

Department of Information and Communications Technology
ICTO-NCC Bldg., CP Garcia Avenue
Diliman, Quezon City

2330 Roxas Blvd., Pasay City. 1300 Philippines

Tel. No. 834 - 4000 L-4-0323-2516

www.dfa.gov.ph

DICT-OSIC/6-442

NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT



UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

HAUT-COMMISSARIAT AUX DROITS DE L'HOMME • OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND

www.ohchr.org • TEL: +41 22 9179400 • FAX: +41 22 917 9038 • registry@ohchr.org

The Office of the United Nations High Commissioner for Human Rights (OHCHR) presents its compliments to all Permanent Missions to the United Nations in Geneva and has the honour to transmit a letter from the Special Rapporteur on the right to freedom of opinion and expression, David Kaye, pursuant to Human Rights Council resolution 25/2.

The Office of the High Commissioner for Human Rights would be grateful if this letter could be transmitted at your earliest convenience to the relevant department or agency, and if the submissions could be sent electronically to freedex@ohchr.org no later than 31 October 2016. Please, to identify your response use the email title "*Submission to study on freedom of expression and the telecommunications and Internet access sector.*"

The Office of the United Nations High Commissioner for Human Rights avails itself of this opportunity to renew the assurances of its highest consideration to all Permanent Missions to the United Nations Office at Geneva.

10 August 2016

NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT



UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

HAUT-COMMISSARIAT AUX DROITS DE L'HOMME • OFFICE OF THE HIGH COMMISSIONER FOR HUMAN RIGHTS
PALAIS DES NATIONS • 1211 GENEVA 10, SWITZERLAND
www.ohchr.org • TEL: +41 22 917 9400 • FAX: +41 22 917 9008 • E-MAIL: freedex@ohchr.org

Mandate of the Special Rapporteur on the promotion of the right to freedom of opinion and expression

9 August 2016

Excellency,

I have the honor to address you in my capacity as United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, pursuant to Human Rights Council resolution 25/2.

Following up on my last report to the Human Rights Council launching a multi-year examination of freedom of expression and the private sector in the digital age, my next report to the Human Rights Council in 2017 will focus on freedom of expression in the telecommunications and Internet access sector. This new report will examine State regulation and action that affect access to telecommunications and Internet networks and services, particularly those provided by Telecommunications and Internet Service Providers. It will also analyse the relevant internal policies and practices of Telcos, ISPs and associated businesses. For more information on the initiative, please see the concept note enclosed.

In this regard, I am presently gathering information on the relevant national legal frameworks and would appreciate receiving information on national norms regulating the following areas:

- 1) *Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) that may permit authorities to require Telecommunications and Internet Service Providers to:*
 - a) *Suspend or restrict access to websites or Internet and telecommunications networks;*
 - b) *Provide or facilitate access to customer data;*
- 2) *Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) on the public disclosure of requests made or actions taken to (a) suspend or restrict access to websites and telecommunications networks and the requests to provide or (b) facilitate access to customer data.*
- 3) *Laws, regulations and other measures (including where applicable contractual arrangements and extra-legal action) governing the activities of private entities that provide network components or related technical support, such as network equipment providers, submarine cable providers, and Internet exchange points;*
- 4) *Remedies available in the event of undue restrictions on Internet and telecommunications access or undue access to customer data*



5) *Other relevant laws, policies or initiatives to promote or enhance Internet accessibility and connectivity, including measures to promote network neutrality.*

I expect to incorporate this information into my report to the 35th Session of the UN Human Rights Council, to be presented in June, 2017.

I wish to thank you in advance for your cooperation and I hope to continue a constructive dialogue on issues related to my mandate. Given the timeliness of this subject, I would respectfully request that any available information be provided, by fax or email (freedex@ohchr.org), not later than 31 October 2016. Please, to identify your response use the email title "*Submission to study on freedom of expression and the telecommunications and Internet access sector.*"

Please accept, Excellency, the assurances of my highest consideration.

David Kaye
Special Rapporteur on the promotion of the right to
freedom of opinion and expression

6/8

The Special Rapporteur also plans to organize expert consultations in October and December 2016 (date and location TBD), aiming for globally representative input and a diverse range of stakeholders, including regulators, private actors, civil society, and the technical community.

Additionally, the Special Rapporteur will identify and engage directly with a small number of relevant business enterprises to deepen his understanding of legal and technical issues from their perspective.

Finally, the Special Rapporteur will continue to examine alleged violations of the right to freedom of opinion and expression in the Telecommunications and Internet Access sector through his regular communications with States and other entities.