Philippines

International cooperation

Specific step-by-step procedures and best practices

Version 21 April 2020

Table of Contents

This information sheet has been prepared by the Cybercrime Programme Office (C-PROC) of the Council of Europe in view of facilitating international cooperation. It does not necessarily reflect official positions of the State covered or of the Council of Europe.

1. Categories of Data (subscriber information, traffic data, content data)

1.1. Definitions under national legislation

Subscriber Information Republic Act No. 10175 or the Cybercrime Prevention Act of 2012	Subscriber's information refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which identity can be established: 1) The type of communication service used, the technical provisions taken thereto and the period of service; (2) The subscriber's identity, postal or geographic address, telephone and other access numbers, any assigned network address, billing and payment information, available on the basis of the service agreement or arrangement; and (3) Any other available information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.
Traffic Data Republic Act No. 10175 or the Cybercrime Prevention Act of 2012	Traffic data or non-content data refers to any computer data other than the content of the communication including, but not limited to, the communication's origin, destination, route, time, date, size, duration, or type of underlying service.
Content Data Implementing Rules and Regulations of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012.	Content data refers to the content of the communication, the meaning or purport of the communication, or the message or information being conveyed by the communication, other than traffic data*; * Also defined under A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants

Back to the Table of Contents

<General comment as to whether Domestic law distinguishes subscriber information from that of traffic and / or content data, whether the same or different rules of procedure apply to obtaining of all types of data>

2. Procedures for preservation requests of stored computer data

2.1 Expedited preservation of stored computer data (Art. 29)

General remarks

Under the Philippine domestic law on cybercrime, which is Republic Act (R.A.) No. 10175 or the Cybercrime Prevention of 2012, preservation of computer data varies as to the type thereof.

For instance, the integrity of subscriber information and traffic data are preserved by the service provider within six (6) months from the date of transaction, while the integrity of the content data are preserved by the service provider within six (6) months from the date of receipt of the preservation request from the law enforcement authorities (LEAs); LEAs may order one (1)-time extension for another six (6) months except when such preserved data are used as evidence in a trial, in which case said data shall be preserved until the termination of the case.

As of date, a service provider located in the Philippines may, on a voluntary basis, directly act on a preservation request coming from LEAs located in other jurisdiction.

Nevertheless, we encourage LEAs located outside the Philippine jurisdiction to direct their request for preservation to the Philippine 24/7 Point-of-Contact (POC) under the purview of the Budapest Convention on Cybercrime, which is:

Name of Institution:	Department of Justice – Office of Cybercrime
Address:	3rd Floor JDC Center, 571 Engracia-Reyes St., Ermita, Manila
Phone number:	+632 8524-8216
Email address:	cybercrime@doj.gov.ph

Urgent requests for preservation are attended to immediately considering that the reason therefor is sufficiently laid down by the requesting LEA.

Back to the Table of Contents

Pursuant to the Budapest Convention on Cybercrime, preservation requests may be denied if the:

a. Request concerns an offense which the requested Party considers a political offence or an offense connected with a political offense, or
b. Requested Party considers that execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests.

Procedures in place

The following procedures are observed by the Department of Justice (DOJ) – Office of Cybercrime (OOC) in dealing with both standard and urgent preservation requests:

Step 1: The DOJ-OOC acknowledges receipt of the request and dockets it in its system.

Step 2: The head of the DOJ-OOC will assign the request to a State Counsel (SC) or an Investigation Agent (IA) as the case may be.

Step 3: The assigned SC or IA will assess the request and see to it that the following information are present:

a. the authority seeking the preservation;
b. the offense that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
c. the stored computer data to be preserved and its relationship to the offense;
d. any available information identifying the custodian of the stored computer data or the location of the computer system;
e. that the requesting LEA/entity intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data; and
f. the urgency of the request, as the case may be.

If the aforesaid information are present, the assigned SC or IA shall draft the necessary Preservation Request addressed to the identified service provider and update the requesting LEA thereof. Otherwise, the DOJ-OOC shall request the requesting LEA for more information.

Step 4: Once the service provider confirms/grants the request, the requesting LEA will be notified accordingly.

Back to the Table of Contents

Step 5: Discuss with the requesting LEA on further steps on how the requested data will be further disclosed.

2.2 Expedited disclosure for stored traffic data (Art. 30)

General remarks

Pursuant to A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants, all types of computer data may only be disclosed when a LEA is equipped with any of these warrants:

a. **Warrant to Disclose Computer Data**

A Warrant to Disclose Computer Data (WDCD) is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of LEAs, authorizing the latter to issue an order to disclose and accordingly, require any person or service provider to disclose or submit computer data in his/her possession or control.[1]

b. **Warrant to Intercept Computer Data**

A Warrant to Intercept Computer Data (WICD) is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of LEAs, authorizing the latter to carry out any or all of the following activities: (a) listening to; (b) recording; (c) monitoring; or (d) surveillance of the content of communications.

This includes the procuring of the content of the computer data at the same time that the communication is occurring, either:

1. Directly, through access and use of a computer system; or
2. Indirectly, through the use of electronic eavesdropping or tapping devices.[2]

c. **Warrant to Search, Seize, and Examine Computer Data**

A Warrant to Search, Seize, and Examine Computer Data (WSSECD) is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of LEAs, authorizing the latter to search the particular place for items to be seized and/or examined.[3]

[1] Section 4.2, Rule on Cybercrime Warrants.
[2] Section 5.2, *Ibid.*
[3] Section 6.1, *Ibid*.

Back to the Table of Contents

The interception of communications and computer data may be conducted during the implementation of the WSSECD: Provided, that:

1. Interception activities shall only be limited to the communications and computer data that are reasonably related to the subject matter of the WSSECD; and
2. Said activities are fully disclosed and explained in the initial return.[4]

d. **Warrant to Examine Computer Data**

A Warrant to Examine Computer Data (WECD) is a warrant authorizing the LEA who has acquired possession of computer device or computer system via a lawful warrantless arrest, or by any other method[5] to conduct forensic examination on the computer data contained therein.[6]

Interception of communications and computer data may likewise be conducted during the implementation of the WECD: Provided, that:

1. Interception activities shall only be limited to the communications and computer data that are reasonably related to the subject matter of the WSSECD; and
2. Said activities are fully disclosed and explained in the initial return.[7]

Procedures in place

The following procedures are observed by the Department of Justice (DOJ) – Office of Cybercrime (OOC) in dealing with both standard and urgent request for disclosure of traffic data:

Step 1: The DOJ-OOC acknowledges receipt of the request and dockets it in its system.
Step 2: The head of the DOJ-OOC will assign the request to a State Counsel (SC) or an Investigation Agent (IA) as the case may be.
Step 3: The assigned SC or IA will assess the request and see to it that the following information are present:

a) The probable offense involved;

[4] Section 6.5, *Ibid*.
[5] Valid warrantless arrest, *en flagrante delicto*, or by voluntary surrender by the unit.
[6] Section 6.9, RCW.
[7] *Supra*, note 22.

Back to the Table of Contents

b) Relevance and necessity of the computer data or subscriber's information sought to be disclosed for the purpose of the investigation;
c) Names of the individuals or entities whose computer data or subscriber's information are sought to be disclosed, including the names of the individuals or entities who have control, possession or access thereto, if available;
d) Particular description of the computer data or subscriber's information sought to be disclosed;[8]
e) Place where the disclosure of computer data or subscriber's information is to be enforced, if available;
f) Manner or method by which the disclosure of the computer data or subscriber's information is to be carried out, if available;[9] and
g) Other relevant information that will persuade the court that there is a probable cause to issue a WDCD.

If the aforesaid information are present, the assigned SC or IA shall draft the necessary endorsement paper to the competent authority, either the National Bureau of Investigation (NBI) or the Philippine National Police (PNP), to facilitate the application of a warrant, and update the requesting LEA thereof. Otherwise, the DOJ-OOC shall request the requesting LEA for more information.

Step 4: The assigned SC/IA on the case shall continue working the request with the competent authority. Once the application is granted and the court issues a warrant, the competent authority shall serve the said warrant against the service provider concerned.

Step 5: The traffic data disclosed by the service provider shall then be disclosed by the competent to the DOJ-OOC, for subsequent endorsement to the requesting LEA.

[8] Ephemeral data: phone calls, short messaging service (SMS), social media internet relay chat (IRC); e-mail or the content data.

[9] E.g., by hard copies or soft copies, by photograph or video, mirror imaging or bit streaming. Bit streaming – refers to making a clone copy of a computer drive. It copies virtually everything included in the drive, including sectors and clusters, which makes it possible to retrieve files that were deleted from the drive. Bit stream images are usually used when conducting digital forensic investigations in a bid to avoid tampering with digital evidence such that it is not lost or corrupted (See http://www.igi-global.com/book/handbook-research-digital-crime-cyberspace/104750), image capture, etc.) [Visited June 3, 2018].

Back to the Table of Contents

3. Procedures for mutual legal assistance

3.1 Requests for stored computer data: subscriber, traffic, content data (Art. 31)

Go to Subscriber information | Traffic Data | Content Data

Requests for subscriber information, traffic data and content data

General remarks

Although Philippine laws provide distinction between types of computer data, the law provides that all types thereof may only be requested from service providers if competent authorities, such as the NBI and PNP are equipped with warrants pursuant to A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants.

The types thereof are adequately discussed under Section 2.2 of this document.

Competent Authorities

Please refer to contact details of the Department of Justice (DOJ) – Legal Staff (Office of the Chief State Counsel) for sending and receiving international cooperation requests, *viz*:

The Secretary
Department of Justice
Padre Faura St., Ermita, Manila 1000
Philippines
Email: ocsc@doj.gov.ph

For Cybercrime cases, please refer to contact details of the DOJ-OOC, which handles international mutual assistance, and supports the Legal Staff in technical aspects, to wit:

Department of Justice – Office of Cybercrime
3rd Floor JDC Center, 571 Engracia-Reyes St., Ermita, Manila
+632 8524-8216

Back to the Table of Contents

cybercrime@doj.gov.ph

Relevant contact points

Please refer to the contact details of the DOJ-OOC in the immediately preceding section of this document.

Prior consultations

Prior consultations may be had with the DOJ-OOC to ensure that incoming requests are in accordance with Philippine laws, rules and regulations. Although this is not a requirement, having prior consultation with the 24/7 POC is highly preferable in order to save time and resources in the facilitation of requests.

Accepted legal basis / mechanisms for MLA requests

i. Laws

Philippine laws that contain provisions on MLA may be used as basis in seeking and providing legal assistance. These laws include Republic Act (R.A.) No. 10175 (Cybercrime Prevention Act of 2012), R.A. No. 9775 (Anti-Child Pornography Act of 2009), and R.A. No. 9160 (Anti-Money Laundering Act), as amended. The Implementing Rules and Regulations of R.A. No. 9208 (Anti-Trafficking in Persons Act of 2003), as amended, also contains provisions on MLA and extradition.

ii. Treaties/Conventions

The Philippines may also seek and provide MLA in criminal matters using as basis the existing bilateral Mutual Legal Assistance Treaties (MLATs) in Criminal Matters.

The Philippines is also a State Party to multilateral treaties that may be used as basis for MLA requests to and from the Philippines (*e.g.*, Convention on Cybercrime or the Budapest Convention, United Nations Convention Against Transnational Organized Crime [UNTOC], ASEAN Mutual Legal Assistance Treaty in Criminal Matters).

iii. Principle of Reciprocity

In the absence of a treaty or law, an MLA request may be made or granted on the basis of the principle of reciprocity provided its execution will not

Back to the Table of Contents

involve coercive action. A Reciprocity Undertaking or an assurance from the requesting State that a similar request for assistance will likewise be granted is required.

Content of the request

A request for MLA shall be in writing and contain the following information -

1. identification of the agency office or authority transmitting the request, as well as the office or authority conducting the investigation, prosecution or related criminal proceeding, including the name and contact details of the person capable of responding to enquiries relating to the request;
2. legal basis for the request;
3. purpose of the request and the nature of the assistance being sought;
4. a statement that the request is made in respect of a criminal matter. The request must establish the connection between the assistance sought and the investigation, prosecution or related criminal proceeding;
5. a description of the facts alleged to constitute the offense and a statement or text of the relevant laws;
6. a description of the offense and the applicable penalty;
7. a description of the evidence, information or other assistance sought;
8. reference to the Preservation Request/Order/Letter previously made by the Requesting Party to the service provider to be served,
9. where necessary, the procedure to be observed in executing the request, including details of the manner and form in which the evidence is to be provided; and
10. any statement on the confidentiality of the request and the reason therefor.

An MLA request may also contain the following information -

1. a description of the documents, records or items of evidence to be produced as well as a description of the appropriate person to be asked to produce them; and
2. any court order relating to the assistance requested and a statement relating to its finality.

Where a request is made on the basis of law or treaty, the requirements thereof are to be complied with.

Certain requests need specific requirements. For example, a request for computer data requires that a request for the preservation of the data be

Back to the Table of Contents

made with the relevant Internet Service Provider prior to submitting the request for assistance.

Applicable legal requirements

Requests for subscriber information, traffic data or content data must be facilitated in accordance with the provisions of A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants, even if there is an existing MLA therefor.

The types thereof are adequately discussed under Section 2.2 of this document.

Confidentiality requirements

Appropriate measures shall be taken to keep confidential MLA requests, its contents and any supporting documents, actions taken pursuant to the request, including the grant of the assistance sought. If disclosure of the request becomes necessary for its execution, the requested State shall so inform the requesting State, which shall then decide whether to pursue its request.

Urgent requests

Appropriate measures shall be taken to keep up with the urgency requirement of an MLA request in line with applicable domestic laws, rules and regulations.

Translation

The MLA requests processed by the Philippine authorities are in the English language. It will be practical if the requests addressed to the Philippine authorities are already translated in the English language so as to conserve time and resources.

Limitations

Any information or evidence obtained through MLA requests shall not be used for any purpose other than for the proceedings stated in the request without the prior consent of the requested jurisdiction.

In addition, the Philippine authorities consider the following as grounds for refusal of a request for assistance, which, depending on the MLAT concerned, may be a mandatory or discretionary ground:

Back to the Table of Contents

1. the request involves an offense regarded by the requested State as being of a political nature or is an offense only under military law;

2. there are substantial grounds for believing that the request for assistance has been made for the purpose of investigating, prosecuting or punishing a person on account of that person's race, sex, religion, nationality, ethnic origin or political opinions, or that person's position may be prejudiced for any of those reasons;

3. the request relates to a person who, if proceeded against in the requested jurisdiction for the offense for which assistance is requested, would be entitled to be discharged on the ground of a previous acquittal or conviction;

4. the execution of the request is likely to prejudice the requested State's sovereignty, security, public order or other essential interests, or is otherwise inconsistent with its domestic law;

5. the provision of assistance would, or would likely, prejudice an investigation, prosecution or related criminal proceeding in the requested State; or

6. the requested State considers that the execution of the request is likely to prejudice its sovereignty, security, public order or other essential interests.

The execution of an MLA request may be postponed if its immediate execution would interfere with any ongoing investigation, prosecution or related criminal proceeding in the requested State.

The requested State is informed of the ground for the refusal or postponement of the execution of the MLA request.

3.2 Requests for real time collection of traffic data (Art. 33)

General remarks

Pursuant to the Supreme Court landmark case of Disini v. The Secretary of Justice[10], the first paragraph of Section 12 of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012 was declared unconstitutional on the

[10] G.R. No. 203335, 11 February 2014.

Back to the Table of Contents

ground that the authority it gives to LEAs is too sweeping and lacks restraint as it curtails civil liberties and provides opportunities for official abuse. It states that, "Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system."

Nevertheless, interception of computer data, as defined under Section 3 (m), Chapter I of Republic Act No. 10175 or the Cybercrime Prevention Act of 2012, may be carried out only by virtue of a court issued warrant, duly applied for by LEAs under Section 5 of A.M. No. 17-11-03-SC or the Rule on Cybercrime Warrants.

Said provision provides for the Warrant to Intercept Computer Data, which is an order in writing issued in the name of the People of the Philippines, signed by a judge, upon application of law enforcement authorities, authorizing the latter to carry out any or all of the following activities: (a) listening to, (b) recording, (c) monitoring, or (d) surveillance of the content of communications, including procuring of the content of computer data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.

Information as to Competent **Authorities**, **Relevant contact points**, **Prior consultations, Accepted legal basis / mechanisms for MLA requests**, **Content of the request, Applicable legal requirements, Confidentiality requirements, Urgent requests, Translation**, and **Limitations** are the same as discussed in Section 3.1 of this document.

3.3 Requests for interception of content data (Art. 34)

Same rules apply as discussed in Section 3.2 of this document.

Back to the Table of Contents