

# **RULE ON CYBERCRIME WARRANTS**

## TABLE OF CONTENTS

	<i>Page</i>
<i>Resolution</i> -----	<i>iii</i>
<b>Section 1. <i>Preliminary Provisions</i></b> -----	1
<b>Section 2. <i>General Provisions</i></b> -----	5
<b>Section 3. <i>Preservation of Computer Data</i></b> -----	8
<b>Section 4. <i>Disclosure of Computer Data</i></b> -----	8
<b>Section 5. <i>Interception of Computer Data</i></b> -----	10
<b>Section 6. <i>Search, Seizure, and Examination of Computer Data</i></b> -----	11
<b>Section 7. <i>Custody of Computer Data</i></b> -----	14
<b>Section 8. <i>Destruction of Computer Data</i></b> -----	16
 <i>Forms</i>	
<b>Annex A. <i>Warrant to Disclose Computer Data</i></b> -----	18
<b>Annex B. <i>Warrant to Intercept Computer Data</i></b> -----	20
<b>Annex C. <i>Warrant to Search, Seize, and Examine Computer Data</i></b> -----	22
<b>Annex D. <i>Warrant to Examine Computer Data</i></b> -----	24



Republic of the Philippines  
Supreme Court  
Manila  
*EN BANC*

A.M. No. 17-11-03-SC

**RESOLUTION**

WHEREAS, Republic Act No. 10175, otherwise known as the “Cybercrime Prevention Act of 2012,” defines acts constituting cybercrime offenses; prescribes penalties therefor; and provides procedures facilitating their detection, investigation, and prosecution;

WHEREAS, the detection, investigation, and prosecution of cybercrime offenses necessitate a rule of procedure therefor, especially for the application, issuance, and implementation of court warrants technically-suited to the nature of cybercrime offenses;

WHEREAS, pursuant to Section 5 (5), Article VIII of the 1987 Constitution, the Supreme Court is vested with the power to promulgate rules concerning the pleading, practice, and procedure in all courts;

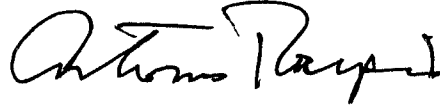
WHEREAS, the Supreme Court, through Memorandum Order No. 11-17 dated February 2, 2017, tasked the Sub-Committee on Commercial Courts to draft the rules of procedure “that shall respond to the technical requirements of cybercrime prosecution and aid the cybercrime courts in the exercise of their special jurisdiction” through a Technical Working Group created for the purpose;

WHEREAS, the Supreme Court, through A.M. No. 17-11-03-SC dated July 3, 2018, approved the Rule on Cybercrime Warrants.

**NOW, THEREFORE**, acting on the recommendation of the Sub-Committee on Commercial Courts, the Court resolved to **APPROVE** the “**Rule on Cybercrime Warrants.**”

The Rule on Cybercrime Warrants shall take effect on August 15, 2018 following its publication in the Official Gazette or in two newspapers of national circulation not later than July 30, 2018.

July 3, 2018




**ANTONIO T. CARPIO**  
Senior Associate Justice


(Per Section 12, Republic Act No. 296,  
The Judiciary Act of 1948, As Amended)



**PRESBITERO J. VELASCO, JR.**  
Associate Justice




**TERESITA J. LEONARDO-DE CASTRO**  
Associate Justice



**DIOSDADO M. PERALTA**  
Associate Justice



**LUCAS P. BERSAMIN**  
Associate Justice




**MARIANO C. DEL CASTILLO**  
Associate Justice



**ESTELA M. PERLAS-BERNABE**  
Associate Justice




**MARVIC M. V. F. LEONEN**  
Associate Justice



**FRANCIS H. JARDELEZA**  
Associate Justice



**ALFREDO BENJAMIN S. CAGUIOA**  
Associate Justice



**SAMUEL R. MARTIRES**  
Associate Justice



**NOEL GIMENEZ TIJAM**  
Associate Justice



**ANDRES B. REYES, JR.**  
Associate Justice



**ALEXANDER G. GESMUNDO**  
Associate Justice

## RULE ON CYBERCRIME WARRANTS<sup>1</sup>

### Section 1. *Preliminary Provisions*

**Section 1.1. *Title.*** – This Rule shall be known and cited as the “Rule on Cybercrime Warrants.”

**Section 1.2. *Scope and Applicability.*** – This Rule sets forth the procedure for the application and grant of warrants and related orders involving the preservation, disclosure, interception, search, seizure, and/or examination, as well as the custody, and destruction of computer data, as provided under Republic Act No. (RA) 10175, otherwise known as the “Cybercrime Prevention Act of 2012.”<sup>2</sup>

**Section 1.3. *Supplementary Nature of this Rule to the Existing Rules of Procedure and Remedies.*** – This Rule supplements the existing Rules of Criminal Procedure, which provisions shall continue to govern the preliminary investigation and all stages of prosecution of criminal actions involving violations of RA 10175, including all crimes defined and penalized by the Revised Penal Code, as amended, and special laws, committed by, through, and with the use of information and communications technologies.

Remedies provided under existing procedural rules shall, whenever applicable, be made available to any party who seeks relief against any of the orders provided under this Rule.<sup>3</sup>

**Section 1.4. *Definition of Terms.*** – For purposes of this Rule:

- a) **Communication** – refers to the transmission of information through information and communications technology (ICT) media, including voice, video, and other forms of data;<sup>4</sup>
- b) **Computer** – refers to an electronic, magnetic, optical, electrochemical, or other data processing or communications device, or grouping of such devices, capable of performing logical arithmetic, routing, or storage functions and which includes any storage facility or equipment or communications

---

<sup>1</sup> “Rule” instead of Rules of Procedure to indicate that the provisions pertain to one set of standards concerning only search, seizure, examination and related processes set forth in the Cybercrime Prevention Act of 2012 (RA 10175). The provisions do not spell out any other procedure of litigating criminal, civil actions or special proceedings. Besides, when one talks about a rule or rules, it already connotes a procedure or set of procedures. Thus, “Rules of Procedure” would be saying the same thing in three words instead of just one word.

<sup>2</sup> Sections 10 to 21, except Sections 12 and 19.

<sup>3</sup> Such remedies as, but not limited to, a motion to quash any of the warrants provided under this Rule.

<sup>4</sup> RA 10175, Chapter 1, Section 3(c); IRR, Rule I, Section 3(g).

facility or equipment directly related to or operating in conjunction with such device;<sup>5</sup>

- c) **Computer data** – refers to any representation of facts, information, or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function, and includes electronic documents and/or electronic data messages whether stored in local computer systems or online;<sup>6</sup>
- d) **Computer system** – refers to any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automated processing of data;<sup>7</sup>
- e) **Content data** – refers to the content of the communication, the meaning or purported meaning of the communication, or the message or information being conveyed by the communication, other than traffic data;<sup>8</sup>
- f) **Cybercrime court** – refers to any of the Regional Trial Courts which are designated as special cybercrime courts;<sup>9</sup>
- g) **Forensic image** – also known as a forensic copy, refers to an exact bit-by-bit copy of a data carrier, including slack, unallocated space, and unused space;<sup>10</sup>
- h) **Forensics** – refers to the application of investigative and analytical techniques that conform to evidentiary standards for use in court;<sup>11</sup>
- i) **Hash value** – refers to the mathematical algorithm produced against digital information (a file, a physical disk or a logical disk) thereby creating a “digital fingerprint” or “digital DNA” for that information;<sup>12</sup>
- j) **Information and Communications Technology (ICT)** – refers to the totality of electronic means to access, create, collect, store,

---

<sup>5</sup> It covers any type of computer device including devices with data processing capabilities like mobile phones, smart phones, computer networks, and other devices connected to the internet; RA 10175, Chapter I, Section 3(d); IRR, Rule I, Section 3(i).

<sup>6</sup> RA 10175, Chapter I, Section 3(e); IRR, Rule I, Section 3(j).

<sup>7</sup> It covers any type of device with data processing capabilities including, but not limited to, computers and mobile phones. The device consisting of hardware and software may include input, output, and storage components which may stand alone or be connected in (*sic*) a network or other similar devices. It also includes computer data storage devices or media; RA 10175, Chapter I, Section 3(g); IRR, Rule I, Section 3(l).

<sup>8</sup> IRR, Rule I, Section 3(m).

<sup>9</sup> A.M. No. 03-03-03-SC, November 15, 2016; RA 10175, Chapter V, Section 21, 2<sup>nd</sup> par.

<sup>10</sup> There are forensic tools available for making these images. Most tools produce information, like hash value, to ensure the integrity of the image; IRR, Rule I, Section 3(w).

<sup>11</sup> Used in, or appropriate for a court of law or other legal context; IRR, Rule I, Section 3(v).

<sup>12</sup> A hash value is a one-way algorithm that makes it impossible to alter digital evidence without causing change in the corresponding values; IRR, Rule I, Section 3(x).

process, receive, transmit, present and disseminate information;<sup>13</sup>

- k) **Interception** – refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content 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;<sup>14</sup>
- l) **Item** – is a general term used to refer to objects of the warrant application and/or the warrant itself, such as the subject computer data, the related computer device/s, and/or other parts of the computer system;
- m) **Offense** – is a general term used to refer to either a violation of Section 4 (Cybercrime Offenses), Section 5 (Other Offenses), or Section 6 (all crimes defined and penalized by the Revised Penal Code, as amended, and other special laws, if committed by, through, and with the use of ICT), Chapter II of RA 10175;
- n) **Off-site search** – refers to the process whereby law enforcement authorities, by virtue of a warrant to search, seize, and examine, are allowed to bring the computer device/s and/or parts of the computer system outside the place to be searched in order to conduct the forensic examination of the computer data subject of the warrant;<sup>15</sup>
- o) **On-site search** – refers to the process whereby law enforcement authorities, by virtue of a warrant to search, seize, and examine, obtains the computer data subject thereof for forensic examination, without the need of bringing the related computer device/s and/or parts of the computer system outside the place to be searched;<sup>16</sup>
- p) **Preservation** – refers to the keeping of data that already exists in a stored form, protected from anything that would cause its current quality or condition to change or deteriorate;<sup>17</sup>

---

<sup>13</sup> RA 10844, Section 3(a).

<sup>14</sup> RA 10175, Chapter I, Section 3(m); IRR, Rule I, Section 3(aa).

<sup>15</sup> “Off-site” search consists of the removal and transportation of the electronic evidence to a location not on the premises and location where the electronic evidence is found or in the location of the area to be searched described in the warrant (Model Code of Cybercrime Investigative Procedure [MCCIP], art. VII, Section 4(f)(I)(A)(iii) and (ii), cited in Brenner, Susan W., and Frederiksen, Barbara A., *Computer Searches and Seizures: Some Unresolved Issues*, p. 65).

<sup>16</sup> “On-site” search is a search conducted on the premises and location where the electronic evidence is found or in the location of the area to be searched described in the warrant (Model Code of Cybercrime Investigative Procedure [MCCIP], art. VII, Section 4(f)(I)(A)(iii) and (ii), cited in Brenner, Susan W., and Frederiksen, Barbara A., *Computer Searches and Seizures: Some Unresolved Issues*, p. 65).

<sup>17</sup> It is the activity that keeps that stored data secure and safe; RA 10175, IRR, Rule I, Section 3(ee).

- q) **Service provider** – refers to: (a) any public or private entity that provides users of its service the ability to communicate by means of a computer system; and (b) any other entity that processes or stores computer data on behalf of such communication service or users of such service;<sup>18</sup>

The term service provider as used in this Rule is understood to include any service provider offering its services within the territory of the Philippines, regardless of its principal place of business;<sup>19</sup>

- r) **Subscriber's information** – refers to any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services, other than traffic or content data, and by which any of the following can be established:

1. The type of communication service used, the technical provisions taken therewith, and the period of service;
2. The subscriber's identity, postal or geographic address, telephone and other access number, any assigned network address, billing and payment information that are available on the basis of the service agreement or arrangement; or
3. Any other available information on the site of the installation of communication equipment that is available on the basis of the service agreement or arrangement;<sup>20</sup> and

- s) **Traffic 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.<sup>21</sup>

## **Section 2. General Provisions**

**Section 2.1. Venue of Criminal Actions.** – The criminal actions for violation of Section 4 (Cybercrime offenses) and/or Section 5 (Other offenses), Chapter II of RA 10175, shall be filed before the designated cybercrime court of the province or city where the offense or any of its elements is committed<sup>22</sup>, or

<sup>18</sup> RA 10175, Chapter I, Section 3(n); IRR, Rule I, Section 3(ff).

<sup>19</sup> Convention on Cybercrime (ETS No. 185), Chapter II, Section 2, Article 18(1)(b).

<sup>20</sup> RA 10175, Chapter I, Section 3(o); IRR, Rule I, Section 3(gg).

<sup>21</sup> RA 10175, Chapter I, Section 3(p); IRR, Rule I, Section 3(hh).

<sup>22</sup> In his comment to the draft Rule on Cybercrime Warrants, Justice Romeo J. Callejo, Sr. (Ret.), Vice Chancellor of the Philippine Judicial Academy and Consultant to the Supreme Court Committee on the Revision of the Rules of Court, pointed out that jurisdiction shall lie if any of the elements of the crime



where any part of the computer system used is situated, or where any of the damage caused to a natural or juridical person took place: *Provided*, that the court where the criminal action is first filed shall acquire jurisdiction to the exclusion of the other courts.<sup>23</sup>

All other crimes defined and penalized by the Revised Penal Code, as amended, and other special laws, committed by, through, and with the use of ICT, as provided under Section 6, Chapter II of RA 10175, shall be filed before the regular or other specialized regional trial courts,<sup>24</sup> as the case may be.

**Section 2.2. *Where to File an Application for a Warrant.*** – An application for a warrant under this Rule concerning a violation of Section 4 (Cybercrime Offenses) and/or Section 5 (Other Offenses), Chapter II of RA 10175 shall be filed by the law enforcement authorities before any of the designated cybercrime courts of the province or the city where the offense or any of its elements has been committed, is being committed, or is about to be committed, or where any part of the computer system used is situated, or where any of the damage caused to a natural or juridical person took place. However, the cybercrime courts in Quezon City, the City of Manila, Makati City, Pasig City, Cebu City, Iloilo City, Davao City and Cagayan De Oro City shall have the special authority to act on applications and issue warrants which shall be enforceable nationwide<sup>25</sup> and outside the Philippines.

On the other hand, an application for a warrant under this Rule for violation of Section 6, Chapter II of RA 10175 (all crimes defined and penalized by the Revised Penal Code, as amended, and other special laws, if committed by, through, and with the use of ICT) shall be filed by the law enforcement authorities with the regular or other specialized regional trial courts, as the case may be, within its territorial jurisdiction in the places above-described.<sup>26</sup>

**Section 2.3. *Incidents Related to the Warrant When a Criminal Action is Instituted.*** – Once a criminal action is instituted, a motion to quash and other incidents that relate to the warrant shall be heard and resolved by the court that subsequently acquired jurisdiction over the criminal action.<sup>27</sup> The prosecution has the duty to move for the transmittal of the records, as well as the transfer of the items' custody to the latter court, which procedure is set forth in Section 7.2 of this Rule.

---

was committed within the Philippines, including its interior and maritime zone, and also outside of its jurisdiction if committed on board a Philippine ship or airship as provided under the Revised Penal Code (Act No. 3815), Article 2(1).

<sup>23</sup> RA 10175, IRR, Rule 4, Section 22.

<sup>24</sup> A.M. No. 99-11-07-SC [February 1, 2000] designates certain branches of the Regional Trial Courts as Family Courts; Supreme Court Administrative Order No. 23-08 [January 23, 2008] designates special courts to hear, try and decide environmental cases;

<sup>25</sup> Expanding the list of SCCCs with authority to issue warrants enforceable nationwide under A.M. No. 03-03-03-SC [November 15, 2016].

<sup>26</sup> The “places above-described” refers to the province or the city where the offense or any of its elements has been committed, is being committed, or is about to be committed, or where any part of the computer system used is situated, or where any of the damage caused to a natural or juridical person took place.

<sup>27</sup> *Malaloan v. Court of Appeals*, G.R. No. 104879, 6 May 1994.

**Section 2.4. Examination of Applicant and Record.** — Before issuing a warrant, the judge must personally examine in the form of searching questions and answers, in writing and under oath, the applicant and the witnesses he may produce, on facts personally known to them and attach to the record their sworn statements, together with the judicial affidavits submitted.

**Section 2.5. Effective Period of Warrants.** – Any warrant issued under this Rule shall only be effective for the length of time as determined by the court, which shall not exceed a period of ten (10) days from its issuance. The court issuing the warrant may, upon motion, extend its effectivity based only on justifiable reasons for a period not exceeding ten (10) days from the expiration of the original period.

**Section 2.6. Contempt.** – Failure to timely file the returns for any of the issued warrants under this Rule or to duly turn-over to the court’s custody any of the items disclosed, intercepted, searched, seized, and/or examined as prescribed hereunder, shall subject the responsible law enforcement authorities to an action for contempt, which procedures shall be governed by Rule 71 of the Rules of Civil Procedure, insofar as they are applicable.

**Section 2.7. Obstruction of Justice for Non-Compliance; Where to File.** — Pursuant to Section 20, Chapter IV of RA 10175, failure to comply with the provisions of Chapter IV, specifically the orders from law enforcement authorities, shall be punished as a violation of Presidential Decree No. 1829, entitled “Penalizing Obstruction Of Apprehension And Prosecution Of Criminal Offenders.”<sup>28</sup>

The criminal charge for obstruction of justice shall be filed before the designated cybercrime court that has jurisdiction over the place where the non-compliance was committed.

**Section 2.8. Extraterritorial Service of Warrants and Other Court Processes.** – For persons or service providers situated outside of the Philippines, service of warrants and/or other court processes shall be coursed through the Department of Justice – Office of Cybercrime, in line with all relevant international instruments and/or agreements on the matter.<sup>29</sup>

---

<sup>28</sup> January 16, 1981; In his comment to the draft Rule on Cybercrime Warrants, Justice Callejo pointed out that the act of non-compliance should be "knowingly or willfully" committed for it to be punishable. This is in accordance with the ruling of the Supreme Court in *Disini, Jr. v. Secretary of Justice*, 727 Phil. 28 [2014].

<sup>29</sup> RA 10175, Chapter VI, Section 22 and Chapter VII, Section 23.

### **Section 3. *Preservation of Computer Data***<sup>30</sup>

**Section 3.1. *Preservation of Computer Data.*** — Pursuant to Section 13, Chapter IV of RA 10175, the integrity of traffic data and subscriber's information shall be kept, retained, and preserved by a service provider for a minimum period of six (6) months from the date of the transaction. On the other hand, content data shall be preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

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

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

### **Section 4. *Disclosure of Computer Data***<sup>31</sup>

**Section 4.1. *Disclosure of Computer Data.*** — Pursuant to Section 14, Chapter IV of RA 10175, law enforcement authorities, upon securing a Warrant to Disclose Computer Data (WDCD) under this Rule, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/her or 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 4.2. *Warrant to Disclose Computer Data (WDCD).*** — A WDCD 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 issue an order to disclose and accordingly, require any person or service provider to disclose or submit subscriber's information, traffic data, or relevant data in his/her or its possession or control.

**Section 4.3. *Contents of Application for a WDCD.*** — The verified application for a WDCD, as well as the supporting affidavits, shall state the following essential facts:

---

<sup>30</sup> RA 10175, Chapter IV, Section 13.

<sup>31</sup> RA 10175, Chapter IV, Section 14.

1. The probable offense involved;
2. Relevance and necessity of the computer data or subscriber's information sought to be disclosed for the purpose of the investigation;
3. 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;
4. Particular description of the computer data or subscriber's information sought to be disclosed;<sup>32</sup>
5. Place where the disclosure of computer data or subscriber's information is to be enforced, if available;
6. Manner or method by which the disclosure of the computer data or subscriber's information is to be carried out, if available;<sup>33</sup> and
7. Other relevant information that will persuade the court that there is a probable cause to issue a WDCD.

**Section 4.4. Issuance and Form of WDCD.** — If the judge is satisfied that there is probable cause to believe that the facts upon which the application for WDCD exists, he/she shall issue the WDCD, which must be substantially in the form prescribed in “Annex A” of this Rule.

**Section 4.5. Return on the WDCD; Retained Copy.** — Within forty-eight (48) hours from implementation or after the expiration of the effectivity of the WDCD, whichever comes first, the authorized law enforcement officer shall submit a return on the WDCD to the court that issued it and simultaneously turn over the custody of the disclosed computer data or subscriber's information thereto as provided under Section 7.1 of this Rule.

It is the duty of the issuing judge to ascertain if the return has been made, and if none, to summon the law enforcement officer to whom the WDCD was issued and require him to explain why no return was made, without prejudice to any action for contempt as provided under Section 2.6 of this Rule.

---

<sup>32</sup> Ephemeral data: phone calls, short messaging service (SMS), social media internet relay chat (IRC); e-mail or the content data.

<sup>33</sup> 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].

Law enforcement authorities are allowed to retain a copy of the disclosed computer data or subscriber's information subject of the WDCD which may be utilized for case build-up or preliminary investigation purposes, without the need of any court intervention; *Provided*, that the details thereof are kept strictly confidential and that the retained copy shall be labelled as such.

The retained copy shall be turned over upon the filing of a criminal action involving the disclosed computer data or subscriber's information to the court where such action has been instituted, or if no criminal action has been filed, upon order of the issuing court under the procedure set forth in paragraph 3 of Section 8.2 of this Rule.

Upon its turn-over, the retained copy shall always be kept, destroyed, and/or returned together with the computer data or subscriber's information that was originally turned over to the issuing court under the first paragraph of this Section.

**Section 4.6. Contempt.** — Non-compliance with the order to disclose issued by law enforcement authorities shall be deemed non-compliance with the WDCD on which the said order is based, and shall likewise give rise to an action for contempt under Section 2.6 of this Rule.

## **Section 5. *Interception of Computer Data***<sup>34</sup>

**Section 5.1. *Interception of Computer Data.*** — Interception, as defined under Section 3 (m), Chapter I of RA 10175, may be carried out only by virtue of a court issued warrant, duly applied for by law enforcement authorities.

**Section 5.2. *Warrant to Intercept Computer Data (WICD).*** — A WICD 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.

**Section 5.3. *Contents of Application for WICD.*** — The verified application for a WICD, as well as the supporting affidavits, shall state the essential facts similar to those in Section 4.3 of this Rule, except that the subject matter is the communication or computer data sought to be intercepted.

---

<sup>34</sup> RA 10175, Chapter IV, Section 15.

**Section 5.4. Issuance and Form of WICD.** — If the judge is satisfied that there is probable cause to believe that the facts upon which the application for WICD exists, he shall issue the WICD, which must be substantially in the form prescribed in “Annex B” of this Rule.

**Section 5.5. Return on the WICD.** — Within forty-eight (48) hours from implementation or after the expiration of the effectivity of the WICD, whichever comes first, the authorized law enforcement officers shall submit a return on the WICD to the court that issued it and simultaneously turn-over the custody of the intercepted communication or computer data thereto as provided under Section 7.1 of this Rule.

It is the duty of the issuing judge to ascertain if the return has been made, and if none, to summon the law enforcement officer to whom the WICD was issued and require him to explain why no return was made, without prejudice to any action for contempt as provided under Section 2.6 of this Rule.

**Section 5.6. Notice after filing of Return.** — Within thirty (30) days from the filing of the return, or, if no return is filed, from the lapse of the forty-eight (48) hour period to file the return, the authorized law enforcement officer has the duty to notify the person whose communications or computer data have been intercepted of the activities conducted pursuant to the WICD. If a return has been filed, a copy of the same shall be attached to the notice. On the other hand, if no return has been filed, the notice shall state the details of the interception activities, including the contents of the intercepted communication or computer data.

Within ten (10) days from notice, the person whose communications or computer data have been intercepted may challenge, by motion, the legality of the interception before the issuing court.

## **Section 6. Search, Seizure and Examination of Computer Data<sup>35</sup>**

**Section 6.1. Warrant to Search, Seize and Examine Computer Data (WSSECD).** — 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 law enforcement authorities, authorizing the latter to search the particular place for items to be seized and/or examined.

**Section 6.2. Contents of Application for a WSSECD.** — The verified application for a WSSECD, as well as the supporting affidavits, shall state the essential facts similar to those in Section 4.3 of this Rule, except that the subject matter is the computer data sought to be searched, seized, and examined, and all other items related thereto. In addition, the application shall

---

<sup>35</sup> RA 10175, Chapter IV, Section 15.

contain an explanation of the search and seizure strategy to be implemented, including a projection of whether or not an off-site or on-site search will be conducted, taking into account the nature of the computer data involved, the computer or computer system's security features, and/or other relevant circumstances, if such information is available.

**Section 6.3. Issuance and Form of WSSECD.** — If the judge is satisfied that there is probable cause to believe that the facts upon which the application for WSSECD exists, he shall issue the WSSECD, which must be substantially in the form prescribed under “Annex C” of this Rule.

**Section 6.4. Off-site and On-site Principle; Return of Items Seized Off-site.** — Law enforcement authorities shall, if the circumstances so allow, endeavor to first make a forensic image of the computer data on-site as well as limit their search to the place specified in the warrant. Otherwise, an off-site search may be conducted, provided that a forensic image is, nevertheless, made, and that the reasons for the said search are stated in the initial return.

A person whose computer devices or computer system have been searched and seized off-site may, upon motion, seek the return of the said items from the court issuing the WSSECD: *Provided*, that a forensic image of the computer data subject of the WSSECD has already been made. The court may grant the motion upon its determination that no lawful ground exists to otherwise withhold the return of such items to him.

**Section 6.5. Allowable Activities During the Implementation of the WSSECD.** — Pursuant to Section 15, Chapter IV of RA 10175, the interception of communications and computer data may be conducted during the implementation of the WSSECD: *Provided*, that the interception activities shall only be limited to communications and computer data that are reasonably related to the subject matter of the WSSECD; and that the said activities are fully disclosed, and the foregoing relation duly explained in the initial return.

Likewise, 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.<sup>36</sup>

**Section 6.6. Initial Return.** — Within ten (10) days from the issuance of the WSSECD, the authorized law enforcement officers shall submit an initial return that contains the following information:

1. A list of all the items that were seized, with a detailed identification of: (a) the devices of the computer system seized, including the name, make, brand, serial numbers, or any other mode of identification, if available; and (b) the hash value of the

<sup>36</sup> RA 10175, Chapter IV, Section 15.

computer data and/or the seized computer device or computer system containing such data;

2. A statement on whether a forensic image of the computer data was made on-site, and if not, the reasons for making the forensic image off-site;
3. A statement on whether the search was conducted on-site, and if not, the reasons for conducting the search and seizure off-site;
4. A statement on whether interception was conducted during the implementation of the WSSECD, together with (a) a detailed identification of all the interception activities that were conducted; (b) the hash value/s of the communications or computer data intercepted; and (c) an explanation of the said items' reasonable relation to the computer data subject of the WSSECD;
5. List of all the actions taken to enforce the WSSECD, from the time the law enforcement officers reached the place to be seized until they left the premises with the seized items and reached the place where the items seized were stored and secured for examination; and
6. A reasonable estimation of how long the examination of the items seized will be concluded and the justification therefor.

It is the duty of the issuing judge to ascertain if the initial return has been made, and if none, to summon the law enforcement authority to whom the WSSECD was issued and require him to explain why no initial return was made, without prejudice to any action for contempt as provided under Section 2.6 of this Rule.

**Section 6.7. *Period to Examine and Order to Return.*** – After the initial return is submitted to the court pursuant to the WSSECD, the court shall issue an order fixing the period to conclude the examination of all the items seized, which period may be extended not exceeding thirty (30) days, upon motion, for justifiable reasons.

**Section 6.8. *Final Return on the WSSECD.*** — Within forty-eight (48) hours after the expiration of the period to examine as provided under Section 6.7 of this Rule, the authorized law enforcement officers shall submit a final return on the WSSECD to the court that issued it, and simultaneously turn-over the custody of the seized computer data, as well as all other items seized and/or the communications or computer data intercepted in relation thereto, following the procedure under Section 7.1 of this Rule.



It is the duty of the issuing judge to ascertain if the final return has been made, and if none, to summon the law enforcement officer to whom the WSSECD was issued and require him to explain why no final return was made, without prejudice to any action for contempt as provided under Section 2.6 of this Rule.

**Section 6.9. Examination where lawful possession of device is obtained; Warrant to Examine Computer Data (WECD).** – Upon acquiring possession of a computer device or computer system via a lawful warrantless arrest, or by any other lawful method,<sup>37</sup> law enforcement authorities shall first apply for a warrant before searching the said computer device or computer system for the purpose of obtaining for forensic examination the computer data contained therein. The warrant therefor shall be denominated as a Warrant to Examine Computer Data (WECD).

The verified application for a WECD, as well as the supporting affidavits, shall state the essential facts similar to those in Section 4.3 of this Rule, except that the subject matter is the computer data sought to be examined. In addition, the application shall disclose the circumstances surrounding the lawful acquisition of the computer device or computer system containing the said computer data.

If the judge is satisfied that there is probable cause to believe that the facts upon which the application for WECD exists, he shall issue the WECD, which must be substantially in the form prescribed under “Annex D” of this Rule.

The initial and final returns, as well as the period to examine under a WECD, shall be similarly governed by the procedures set forth in Sections 6.6 to 6.8 of this Rule.

Interception of communications and computer data may be likewise conducted during the implementation of the WECD under the same conditions stated in Section 6.5 of this Rule.

## **Section 7. Custody of Computer Data**

**Section 7.1. Deposit and Custody of Seized Computer Data.**<sup>38</sup> — Upon the filing of the return for a WDCD or WICD, or the final return for a WSSECD or WECD, all computer data subject thereof shall be simultaneously deposited in a sealed package with the same court that issued the warrant. It shall be accompanied by a complete and verified inventory of all the other items seized in relation thereto, and by the affidavit of the duly authorized law enforcement officer containing:

---

<sup>37</sup> Valid warrantless seizure, *en flagrante delicto*, or by voluntary surrender of the unit.

<sup>38</sup> RA 10175, Chapter IV, Section 16.

1. The date and time of the disclosure, interception, search, seizure, and/or examination of the computer data, as the case may be. If the examiner or analyst has recorded his/her examination, the recording shall also be deposited with the court in a sealed package and stated in the affidavit;
2. The particulars of the subject computer data, including its hash value;
3. The manner by which the computer data was obtained;
4. Detailed identification of all items seized in relation to the subject computer data, including the computer device containing such data and/or other parts of the computer system seized, indicating the name, make, brand, serial numbers, or any other mode of identification, if available;
5. The names and positions of the law enforcement authorities who had access to the computer data from the time of its seizure until the termination of the examination but prior to depositing it with the court,<sup>39</sup> and the names of officers who will be delivering the seized items to the court;<sup>40</sup>
6. The name of the law enforcement officer who may be allowed access to the deposited data. When the said officer dies, resigns or severs tie with the office, his/her successor may, upon motion, be granted access to the deposit; and
7. A certification that no duplicates or copies of the whole or any part thereof have been made, or if made, all such duplicates or copies are included in the sealed package deposited, except for the copy retained by law enforcement authorities pursuant to paragraph 3 of Section 4.5 of this Rule.

The return on the warrant shall be filed and kept by the custodian of the log book on search warrants who shall enter therein the date of the return, the description of the sealed package deposited, the name of the affiant, and other actions of the judge.

**Section 7.2. *Duty of the Prosecutor When Criminal Action is Instituted.*** – Once a criminal action is instituted, it shall be the duty of the prosecutor, or his/her duly authorized representatives, to move for the immediate transmittal of the records as well as the transfer of the intercepted, disclosed, searched, seized and/or examined computer data and items, including the complete and verified inventory thereof, to the court that subsequently acquired jurisdiction over the criminal action. The motion for the purpose shall be filed before the

---

<sup>39</sup> Temporary custody.

<sup>40</sup> Chain of custody.

court that issued the warrant and has custody of the computer data within ten (10) days from the time the criminal action is instituted and shall be acted upon by the court within a period of five (5) days.

**Section 7.3. Access to and Use of Computer Data.**<sup>41</sup> — The package containing the computer data so deposited under Section 7.1 of this Rule shall not be opened, or the recordings replayed, or its contents revealed, or, in any manner, used as evidence,<sup>42</sup> except upon motion duly granted by the court. The motion for the purpose shall state:

1. The relevance of the computer data sought to be opened, replayed, revealed, or used as evidence; and
2. The names of the persons who will be allowed to have access thereto, if the motion is granted.

The motion shall further include proof of service of copies sent to the person or persons whose computer data is the subject of the motion. The said person or persons shall be given ten (10) days from receipt of notice thereof to file a comment, after which the court shall rule on the motion, unless it finds it necessary to conduct a clarificatory hearing for the purpose.

## **Section 8. Destruction of Computer Data**<sup>43</sup>

**Section 8.1. Duty of Service Providers and Law Enforcement Authorities to Destroy.** — Pursuant to Section 17 of RA 10175, upon expiration of the periods as provided in Sections 13 and 15 of the said law, service providers and law enforcement authorities, as the case may be, shall immediately and completely destroy the computer data subject of preservation and examination.

**Section 8.2. Destruction and Return of Computer Data in the Custody of the Court.** — Upon motion and due hearing, the court may, for justifiable reasons, order the complete or partial destruction, or the return to its lawful owner or possessor, of the computer data or any of the related items turned over to its custody.

---

<sup>41</sup> RA 10175, Chapter IV, Section 16.

<sup>42</sup> In his comment to the draft Rule on Cybercrime Warrants, Justice Callejo pointed out that the construction of the phrase “used as evidence” can be in reference to the offense for which the warrant was applied or to a different offense altogether. The latter instance may fall under the doctrine of “independent source of evidence”, which allows for the introduction of evidence obtained by a separate and distinct method, an independent source; cited in Bloom, Robert M., *Inevitable Discovery: An Exception beyond the Fruits* (1992), 20 Am. J. Crim. L. 079.

<sup>43</sup> RA 10175, Section 17 uses the word “destroy” in reference to the preserved “traffic data, subscriber information, content data” under Sec. 13 and searched, seized & examined “computer data” under Sec. 15 of RA 10175. The described types of information, however, being essentially electronically stored information (ESI) cannot easily lend themselves to “destruction”, thus, the use of the words remove and delete in tandem with “destroy”. The word “destroy” cannot be omitted because RA 10175 employs it. It may be inappropriate for a rule to change a material word in the law.

Likewise, the court may, *motu proprio*, and upon written notice to all the parties concerned, order the complete or partial destruction, or return to its lawful owner or possessor, of the computer data or any of the related items turned over to its custody if no preliminary investigation or case<sup>44</sup> involving these items has been instituted after thirty-one (31) days from their deposit, or if preliminary investigation has been so instituted within this period, upon finality of the prosecutor's resolution finding lack of probable cause. In its sound discretion, the court may conduct a clarificatory hearing to further determine if there is no reasonable opposition to the items' destruction or return.

If the court finds the destruction or return of disclosed computer data or subscriber's information subject of a WDCD to be justified under this Section, it shall first issue an order directing the law enforcement authorities to turn-over the retained copy thereof as described in paragraph 3 of Section 4.5 of this Rule. Upon its turn-over, the retained copy shall be simultaneously destroyed or returned to its lawful owner or possessor together with the computer data or subscriber's information that was originally turned over to the issuing court.

**Section 8.3. Destruction of Computer Data; How Made.** — The destruction of computer data and related items, if so allowed under Section 8.2 of this Rule, shall be made in the presence of the Branch Clerk-of-Court, or in his/her absence, in the presence of any other person duly designated by the court to witness the same. The accused or the person/s from whom such items were seized, or his/her representative or counsel, as well as the law enforcement officer allowed access to such items as indicated in the inventory, or his/her duly authorized representative, may also be allowed to witness the said activity; *Provided*, that they appear during the scheduled date of destruction upon written notice to them by the Branch Clerk-of-Court at least three (3) days prior to the aforementioned date.

Within twenty-four (24) hours from the destruction of the computer data, the Branch Clerk-of-Court or the witness duly designated by the court shall issue a sworn certification as to the fact of destruction and file the said certificate with the same court.

The storage device, or other items turned over to the court's custody, shall be destroyed by shredding, drilling of four holes through the device, prying the platters apart, or other means in accordance with international standards that will sufficiently make it inoperable.

x ----- e n d ----- x

---

<sup>44</sup> Refers to criminal actions where preliminary investigation is not required as provided under Section 1, Rule 112 in relation to Section 1, Rule 110 of the Rules of Criminal Procedure.

**Annex A – Warrant to Disclose Computer Data.**

Republic of the Philippines  
Regional Trial Court  
Branch \_\_, \_\_\_\_\_

*Re: Application for a Warrant to Disclose  
Computer Data under Section 14  
of Republic Act No. 10175*

WDCD No. \_\_\_\_\_

**NAME OF APPLICANT,**  
Applicant.

X-----X

**WARRANT TO DISCLOSE COMPUTER DATA**

To the law enforcement authorities:

Greetings:

It appearing to the satisfaction of the undersigned after examining under oath (*name of applicant*) and his/her witness/es (*name/s of witness/es*) that there is probable cause to believe that (*state the probable offense involved*) has been committed, is being committed or is about to be committed, a Warrant to Disclose Computer Data (WDCD) is hereby **ISSUED**, in accordance with the provisions of Section 4 of A.M. No. \_\_, entitled the “Rule on Cybercrime Warrants”.

**WHEREFORE**, by virtue of this WDCD, you are hereby **AUTHORIZED** to issue an order compelling (*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*) to disclose or submit (*particular description of the computer data or subscriber’s information sought to be disclosed*).

*(In the judge’s discretion, indicate other terms to be included by the law enforcement authorities in the order to disclose, as may be gathered from the warrant application, such as the place where the disclosure is to be enforced, the manner or method by which the disclosure is to be carried out, and other relevant terms to attend the implementation of the order to disclose, subject to the limitations imposed by law.)*

The authorized law enforcement officer is **COMMANDED** to submit a return on the WDCD and simultaneously turn-over the custody of the disclosed computer data or subscriber’s information to the undersigned within

the period and under the terms prescribed in the Rule on Cybercrime Warrants.

Fail not under penalty of law.

Witness my hand this \_\_\_ day of \_\_\_, in the City \_\_\_, Philippines

---

**ISSUING JUDGE**

**Annex B – Warrant to Intercept Computer Data.**

Republic of the Philippines  
Regional Trial Court  
Branch \_\_, \_\_\_\_\_

*Re: Application for a Warrant to Intercept  
Computer Data under Section 15 in relation  
to Section 3(m) of Republic Act No. 10175*

WICD No. \_\_\_\_\_

**NAME OF APPLICANT,**

Applicant.

x-----x

**WARRANT TO INTERCEPT COMPUTER DATA**

To the law enforcement authorities:

Greetings:

It appearing to the satisfaction of the undersigned after examining under oath (*name of applicant*) and his/her witness/es (*name/s of witness/es*) that there is probable cause to believe that (*state the probable offense involved*) has been committed, is being committed or is about to be committed, a Warrant to Intercept Computer Data (WICD) is hereby **ISSUED**, in accordance with the provisions of Section 5 of A.M. No. \_\_, entitled the “Rule on Cybercrime Warrants”.

**WHEREFORE**, by virtue of this WICD, you are hereby **AUTHORIZED** to listen to, record, monitor, and/or conduct surveillance of (*particular description of the communications and/or computer data sought to be intercepted*), which are communications or computer data of (*names of the individuals or entities whose communication or computer data are sought to be intercepted, including the names of the individuals or entities who have control, possession or access thereto, if available*).

*(In the judge’s discretion, indicate other terms to attend the implementation of the WICD as may be gathered from the warrant application, such as the place where the interception is to be enforced, the manner or method by which the interception is to be carried out, and other relevant terms, subject to the limitations imposed by law.)*

The authorized law enforcement officer is **COMMANDED** to submit a return on the WICD and simultaneously turn-over the custody of the intercepted communication or computer data to the undersigned, as well as notify the person whose communications or computer data have been

intercepted of the activities conducted pursuant to this warrant, within the periods and under the terms prescribed in the Rule on Cybercrime Warrants.

Fail not under penalty of law.

Witness my hand this \_\_\_\_ day of \_\_\_\_, in the City \_\_\_\_, Philippines

---

**ISSUING JUDGE**



**Annex C – Warrant to Search, Seize, and Examine Computer Data.**

Republic of the Philippines  
Regional Trial Court  
Branch \_\_, \_\_\_\_\_

*Re: Application for a Warrant to Search, Seize, and Examine Computer Data under Section 15 of Republic Act No. 10175*      WSSECD No. \_\_\_\_\_

**NAME OF APPLICANT,**  
Applicant.  
x-----x

**WARRANT TO  
SEARCH, SEIZE, AND EXAMINE COMPUTER DATA**

To the law enforcement authorities:

Greetings:

It appearing to the satisfaction of the undersigned after examining under oath (*name of applicant*) and his/her witness/es (*name/s of witness/es*) that there is probable cause to believe that (*state the probable offense involved*) has been committed, is being committed or is about to be committed, a Warrant to Search, Seize, and Examine Computer Data (WSSECD) is hereby **ISSUED**, in accordance with the provisions of Section 6 of A.M. No. \_\_, entitled the “Rule on Cybercrime Warrants”.

**WHEREFORE**, by virtue of this WSSECD, you are hereby **AUTHORIZED** to search, seize, and examine (*particular description of the computer data sought to be searched, seized, and examined, and all other items related thereto*), which are computer data and/or items of (*names of the individuals or entities whose computer data and/or items are sought to be searched, seized, and examined, including the names of the individuals or entities who have control, possession or access thereto, if available*), as well as conduct the allowable activities stated in Section 6.5 of the Rule on Cybercrime Warrants during the implementation of this warrant.

*(In the judge’s discretion, indicate other terms to attend the implementation of the WSSECD as may be gathered from the warrant application, such as the place where the search and seizure is to be enforced, the search and seizure strategy to be implemented, including a projection of whether or not an off-site or on-site search will be conducted, taking into account the nature of the computer data involved, the computer or computer system’s security features, and/or other relevant circumstances, if such*

*information is available, and other relevant terms, subject to the limitations imposed by law.)*

The authorized law enforcement officer is **COMMANDED** to submit an initial return, and thereafter, a final return on the WSSECD together with the simultaneous turn-over of the custody of the items searched, seized, and examined pursuant to this warrant, within the periods and under the terms prescribed in the Rule on Cybercrime Warrants.

Fail not under penalty of law.

Witness my hand this \_\_\_ day of \_\_\_, in the City \_\_\_\_, Philippines

---

**ISSUING JUDGE**

**Annex D – Warrant to Examine Computer Data.**

Republic of the Philippines  
Regional Trial Court  
Branch \_\_, \_\_\_\_\_

*Re: Application for a Warrant to Examine  
Computer Data under Section 15 of  
Republic Act No. 10175*

WECD No. \_\_\_\_\_

**NAME OF APPLICANT,**

Applicant.

X-----X

**WARRANT TO EXAMINE COMPUTER DATA**

To the law enforcement authorities:

Greetings:

It appearing to the satisfaction of the undersigned after examining under oath (*name of applicant*) and his/her witness/es (*name/s of witness/es*) that the possession of the computer device or computer system as particularly described below has been lawfully acquired, and that there is probable cause to believe that (*state the probable offense involved*) has been committed, is being committed or is about to be committed, a Warrant to Examine Computer Data (WECD) is hereby **ISSUED**, in accordance with the provisions of Section 6 of A.M. No. \_\_\_\_, entitled the “Rule on Cybercrime Warrants”.

**WHEREFORE**, by virtue of this WECD, you are hereby **AUTHORIZED** to search (*particular description of the computer device or computer system containing the computer data sought to be examined*), which possession was acquired via (*state the circumstances surrounding the lawful acquisition of the computer device or computer system*), and thereafter, obtain (*particular description of the computer data sought to be examined*) for the conduct of forensic examination, as well as intercept communications and computer data during the implementation of the WECD under the same conditions stated in Section 6.5 of the Rule on Cybercrime Warrants.

*(In the judge’s discretion, indicate other terms to attend the implementation of the WECD as may be gathered from the warrant application, such as the place where the search of the computer device or computer system, and the subsequent examination of the computer data contained therein are to be conducted, and other relevant terms, subject to the limitations imposed by law.)*

The authorized law enforcement officer is **COMMANDED** to submit an initial return, and thereafter, a final return on the WECD together with the simultaneous turn-over of the custody of the items searched and examined pursuant to this warrant, within the periods and under the terms prescribed in the Rule on Cybercrime Warrants.

Fail not under penalty of law.

Witness my hand this \_\_\_ day of \_\_\_, in the City \_\_\_, Philippines

---

**ISSUING JUDGE**