Republic of the Philippines
National Police Commission
NATIONAL HEADQUARTERS, PHILIPPINE NATIONAL POLICE
DIRECTORATE FOR INVESTIGATION AND DETECTIVE MANAGEMENT
Camp BGen Rafael T Crame, Quezon City

DEC 0 4 2017

Investigative Directive No. 2017 - 17

Directive on the Referral and Conduct of Digital Forensic Examination

1. REFERENCES:

a. Republic Act No. 10175 otherwise known as the "Cybercrime Prevention Act of 2012";
b. Police Operational Procedure (POP) Revised 2013;
c. NAPOLCOM Memorandum Circular 2013-220 entitled "Approving the Activation of the Philippine National Police Anti-Cybercrime Group as a National Support Unit";
d. The Revised Rules on Criminal Procedures;
e. DOJ Legal Opinion No. LML-L-25H15-982 dated August 25, 2015; and
f. DIDM IMPLAN re PNP Anti-Illegal Drugs Campaign Plan Project: "Double Barrel".

2. BACKGROUND:

The Anti-Cybercrime Group (ACG), created pursuant to Republic Act 10175, is rresponsible for the efficient and effective enforcement of its provisions[1]. Under the law and its Implementing Rules and Regulations, one of the functions of the ACG is to *conduct data recovery and forensic analysis on computer systems and other electronic evidence seized.*[2] These functions are also substantially laid down in NAPOLCOM Memorandum Circular 2013-220 and its PNP implementing orders, which mandates the ACG to perform the following tasks,[3] among others:

- *Conduct data recovery and forensic analysis on all computers, computer peripherals and storage devices, and other digital evidence seized by PNP units and any other law enforcement agencies within the country.*

- *Provide operational support to investigative units within the PNP, including the search, seizure, evidence preservation, and forensic examination of all digital evidence from crime scenes.*

- *Formulate guidelines for Cybercrime investigation, forensic evidence recovery and forensic data analysis.*

[1] Section 10, RA 10175
[2] Section 10, IRR of RA 10175
[3] NAPOLCOM Resolution No. 2013-220, February 27, 2013 and General Order No. DPL-12-09

To accomplish these tasks, the ACG maintains a Digital Forensic Laboratory (DFL) in the National Headquarters, and deploys Digital Forensic Examiners to its various field units/offices to provide technical assistance to cybercrime investigators and other operating units of the PNP, whenever it is alleged that a computer or computer system is used in the commission of the crime, or is the object of a cybercrime.

Since the ACG's creation up to the present, the DFL receives numerous requests from various PNP units for the conduct of digital forensic examinations on seized or recovered computers, computer systems, and storage devices.

Although the ACG understands that it is mandated to conduct *data recovery and forensic analysis on all computers, computer peripherals and storage devices, and other digital evidence seized by PNP units*, it is also aware that this obligation must be exercised with regard and consideration to established rules and legal procedures.

A review of the requests from other units would reveal that the devices referred for digital forensic examination were recovered from either of the following kinds of police operations:

1) Pursuant to a Search Warrant for cybercrime or cyber-enabled crime, where computer and other digital devices are the objects to be searched;
2) Pursuant to a Search Warrant for a traditional crime, where computer and other digital devices are not included as objects to be searched;
3) Seized through search incidental to a lawful arrest for a cybercrime or cyber-enabled crime;
4) Seized through search incidental to a lawful arrest for a traditional crime; or
5) From scenes of the crime during the conduct of police investigation.

3. RATIONALE:

The **right** of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures, and their **right** to privacy of communications and correspondence, are rights protected by no less than the Philippine Constitution. The right to privacy to one's affairs may be inferred in the ban against unreasonable search and seizure and the prohibition against self-incrimination.

In recognition of these rights, certain laws, the Revised Rules on Criminal Procedures, the PNP Police Operational Procedure, and various jurisprudence had laid down sufficient parameters to guide state agents in ensuring that state action does not result to violation of any of the foregoing rights, and that evidence obtained are admissible in evidence in any judicial or quasi-judicial proceedings.

Established is the general rule that search and seizure requires court warrant, and that a search without a warrant may only be made in exceptional circumstances, such as when a person is lawfully arrested, and he has in his possession dangerous weapons or anything which may have been used or constitute proof in the commission of an offense[4]. The rules were clear until the advent of information and communications technology (ICT) produced a new type of evidence: *Digital Evidence.*

Unlike obtaining traditional evidence, the gathering of digital information is carried out by the search and examination of the contents of a digital device, the tapping or surveillance of network traffic, the interception of intangible communications, or the making of digital copies. The search and seizure of digital evidence has thus created a new forensic field in law enforcement investigation and prosecution, known as *Digital Forensics.*

The advent of digital evidence raised a number of questions, like, to what extent and circumstances may the police conduct a warrantless search of the contents of a person's mobile device upon a person's arrest? If the rules provide for the conduct of routine search after a valid warrantless arrest, does this search extend to the contents of the digital device seized from the arrested person in a forensic laboratory?

4. PURPOSE

This Investigative Directive prescribes the requirements to be observed by all PNP units in referring seized digital devices to the PNP ACG or in requesting for technical assistance for the conduct of digital forensic examination and analysis. The procedures and principles shall ensure that digital evidence is gathered in a manner that is admissible in any judicial, administrative or quasi-judicial bodies and the chain of custody is observed.

5. GENERAL GUIDELINES:

The following laws and rules established guidelines in determining proper law enforcement conduct in the search and seizure of digital evidence:

1) Republic Act No. 10175 or the "Cybercrime Prevention Act"

Under Section 15, search and seizure warrant is required before law enforcement authorities may conduct forensic analysis or examination. It states that:

> **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.

[4] Section 13 of Rule 126, Revised Rules on Criminal Procedure

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.

Section 18 discusses the consequence when evidence is obtained without observing the rule laid down above, which is also a general principle in law:

> **Section 18.** *Exclusionary Rule.* — Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

2) Police Operational Procedures Revised 2013

The PNP POP Revised 2013 has also echoed the same principle laid down under RA No. 10175. It dedicated an entire rule on Cybercrime Incident Response Procedure under Rule 36. In order to highlight the procedure, it is imperative to quote some pertinent rules on the search and seizure of data from digital devices:

36.2 Guidelines for Cybercrime Incident First Responder

1) When responding to a cybercrime incident, or to a scene of the crime where computers *(or electronic device, digital media, and other similar devices)* are present, it is imperative for the First Responder (FR) to be able to protect, seize, and search the same and to be able to recognize potential evidence, using the following questions as guidelines to determine its role in the commission of the crime:

    (1) Is it a contraband or fruit of a crime?
    (2) Is it a tool used for the commission of the crime?
    (3) Is it only incidental to the crime, i.e. being used to store evidence of the crime?
    (4) Is it both instrumental to the crime and a storage device for evidence?

2) After identifying the theories as to the role of the computer in the commission of the crime, the following questions essential to any further police intervention should be considered by the first responder:

   (1) Is there probable cause to seize the hardware?
   (2) Is there probable cause to seize the software?
   (3) Is there probable cause to seize the data?
   (4) Where will the search and seizure be conducted?

3) Search of computers *(or electronic device, digital media, and other similar devices)* and seizure of data therefrom **require a warrant issued by the court.** (emphasis supplied)
4) Appropriate collection techniques shall be used to preserve the data sought to be seized.
5) The evidence seized shall be subjected to forensic examination by trained personnel. The result of the forensic examination, as well as the testimony of the forensic expert, shall be made available during the trial.

36.4 Guidelines in the Treatment of Other Electronic Data Storage Devices

The FR should understand that other electronic devices may contain viable evidence associated with the crime. The FR must ensure that, **unless an emergency exists**, the device should not be accessed. Should it be necessary to access the device, the FR should ensure that all actions associated with the manipulation of the device should be noted in order to document the chain of custody and ensure its admission as evidence in court.

To summarize, under the Cybercrime Prevention Act, one of the methods[5] of obtaining digital evidence is through the implementation of a search and seizure warrant. When a search and seizure is issued for a cybercrime offense, the operating team is now vested with the authority to conduct forensic examination, analysis and interception of a digital device or a communication, among others, during the life of the warrant.

This is the same principle laid down in the Police Operational Procedures as stated above. The POP states that search and seizure of computers requires a warrant, unless **an emergency exists.** Emergency or exigent circumstance has long been recognized as exception to the general rule of the necessity of a warrant before a search can be made. Emergency circumstance as exception includes those circumstances when police officers have reasonable ground to believe that a crime was being committed, however, they have no opportunity to apply for a search warrant from the courts because the latter were closed[6].

---

[5] Another method is through the preservation, disclosure of data and interception under Section 13, 14, and 15 of RA 10175

[6] People v. De Gracia, G.R. Nos. 102009-10, July 6, 1994

3) Exigent Circumstance as culled from People vs. Enojas[7] (with discussion of *Riley v. California*[8])

In this case, Enojas was stopped by police officers when he suspiciously parked his taxi in front of a store. He was invited by the officers to go with them to the police station. On their way, the officers apprehended two robbers who exchanged gunshots with them, killing an officer. Enojas fled the scene.

The officers searched Enojas' abandoned car and found his mobile phone. They monitored the text messages on the phone and communicated with the other suspects, resulting to an entrapment operation. Enojas, along with the other suspects, were charged for murder.

The Court found that the text messages were properly admissible because the police officer, posing as Enojas, had personal knowledge of the messages and was competent to testify about them.

The search and seizure of information without a warrant under exigent circumstances is also recognized as an exception to the general rule in the latest American jurisprudence of *Riley v. California*[9], where the US Supreme Court had the occasion to distinguish search incidental to a lawful arrest vis-à-vis extensive search of a digital device, in this manner:

> "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Officers may examine the phone's physical aspects to ensure that it will not be used as a weapon, but the data on the phone can endanger no one. To the extent that a search of cell phone data might warn officers of an impending danger, e.g., that the arrestee's confederates are headed to the scene, such a concern is better addressed through consideration of case-specific exceptions to the warrant requirement, such as exigent circumstances."

---

[7] G.R. No. 204894, March 10, 2014
[8] 573 US _2014
[9] *Supra.*

6. SPECIFIC GUIDELINES

R.A. No. 10175 states that the ACG[10] shall exclusively handle cases involving violations of the law. This means that cybercrimes, particularly defined in Section 4, shall be exclusively investigated by the ACG. However, other units may avail of the conduct of digital forensic examinations (and other authorities under Section 15 of RA No. 10175) for violations under Revised Penal Code (RPC) and other special laws, when it is alleged that the commission is by, through, and with the use of ICT.

The PNP ACG Digital Forensic Laboratory (DFL) shall conduct digital forensics examination and analysis on computers and other digital devices referred by other PNP units, either through technical assistance during the implementation of the warrant or in the laboratory, provided the following requirements are observed:

a. Search Warrant for an ICT-Enabled Crime

1) The request for technical assistance shall be signed by the head of office and accompanied by a copy of the Warrant which indicates in the title that it was issued for an offense committed through ICT;

2) A Pre-Operational Coordination addressed to the Director, ACG or his authorized representatives shall be submitted at least three days prior to the implementation of the Warrant;

3) The conduct of forensic examination shall be valid during the life of the search warrant, which is ten (10) days from issuance;

4) If the on-site forensic examination is not yet complete, but the life of the warrant has already expired or the warrant was returned to court, the implementing unit shall request the court, upon the return of the warrant or the expiration of the 10-day period, for an extension of time to conduct digital forensic examination, and to issue orders directing the ACG to conduct the same;

5) Upon securing the said Court Order, the head of office, through the investigator-on-case and/or the evidence custodian, shall make a request to the ACG for the conduct of further examination, attaching the Court Order and enumerating therein the kind of digital evidence to be searched and examined by the forensic personnel;

[10] To include the Cybercrime Division of the NBI

6) The above request shall be accompanied by a destination/hard drive, which shall be at least twice the memory of the device being examined;

7) Before the lapse of the period of examination, the requesting unit/office shall coordinate with the DFL, through any means of communication, whether the examination may be complete before the lapse of the period given by the court. If the examination cannot be completed within the time provided in the Order, the requesting party shall make a Motion to the court for the extension of time to complete the examination;
8) Once the examination is complete, all data shall, within forty-eight (48) hours after the expiration of the time to conduct digital forensic examination, be deposited with the Issuing Court, if no criminal action has been instituted, otherwise, it shall be deposited with the Hearing Court;

9) The data shall be in a sealed package, and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data;

10) The law enforcement authority shall also certify that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court; and

11) The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or the contents revealed, except upon order of the court.

b. Search Warrant for Traditional Crimes

The digital forensic examination of computers or devices confiscated by PNP unit pursuant to the implementation of a search warrant for traditional crimes shall only be made when there is a court order directing the ACG to conduct the same, even if computers or devices were listed as items to be seized in the search warrant.

c. Search and Seizure Incidental to a Lawful Arrest

1) When the warrantless arrest of a suspect is pursuant to a cybercrime or ICT-enabled crime, the arresting officers may conduct a thorough search of his person, to include the confiscation of the device believed to have been used in the commission of an offense. Under exigent circumstances, the contents of the device may be searched by the personnel themselves *contemporaneous* to the arrest, or they may opt

2) to seek, as soon as the exigency of the circumstance becomes apparent, for technical assistance from the ACG;

3) The request shall be made, as much as possible, through a written request; however, if the said written request will defeat the purpose of examination, other forms of communications available to the PNP (use of official mobile numbers and emails) may be made, by the head of office to the Director of the ACG or his representatives; and

4) In cases where exigency is not present, the examination shall only be made when there is an Order from a competent court directing the ACG to conduct the said examination, following the other requirements discussed above.

d. Consented Search

1) When a crime is under investigation of a PNP unit, and the complainant or his witness desires that the police examine a legally owned computer or device in order to obtain evidence therefrom, the investigator-on-case shall cause the owner to sign a Consent to Search form, and attach the same to the unit's request to the ACG. In cases where the legal owner is deceased, the consent form shall be accomplished by the spouse or any direct family member.

2) In case of minors, consent shall be conformed by the parents or guardians, or in their absence, the DSWD or LSWDO as the case may be.

3) For requests coming from partners and other stakeholders, digital forensic examination may be extended to them provided it can be shown that the digital device is voluntarily submitted and there is legal purpose for the examination, recovery or preservation of data.

e. CCTV Examination and Enhancement

1) In cases where the request is for the enhancement of CCTV footage/s, a document showing consent of the CCTV owner shall be attached to the request.

f. Other Forms

1) When a digital or electronic device is recovered in a crime scene, and the owner thereof is dead, digital forensic examination may be made without a Court warrant. The requesting PNP unit shall specify in the request the type of information or data that shall be searched and seized.

2) When the owner of an electronic or digital device recovered from the crime scene is unknown or unidentified, the investigating unit shall obtain a search warrant from the court directing the ACG to conduct digital forensic examination on the device.

3) The search and seizure of government-issued computer or device to a public employee may be searched without a warrant[11], provided it is shown that (a) the employee cannot have any reasonable expectation of privacy under the circumstances; and (b) the scope of the intrusion requested by the government agency is reasonable.

4) In requests for digital forensic examinations of computers owned by companies, pursuant to a criminal investigation conducted by a PNP unit, the company, through an authorized representative, shall issue a certification that the computer or device so requested for examination is owned by the company and company policy states that the user thereof does not expect privacy over said device.

7. ADDITIONAL GUIDELINES

a. All requests for technical assistance to the ACG shall be signed by the concerned unit commander/chief.

b. The ACG reserves its right not to receive any electronic devices submitted for digital forensic analysis or examination, if upon initial evaluation/assessment, the said device(s) is/are beyond the capability of the digital forensic laboratory to examine.

c. The ACG DFL shall notify the requesting party once the examination and analysis of the digital device is already complete. Upon notification, the requesting party shall have 45 days to claim the result of examination. If, after the expiration of the 45-day period from notification, the requesting party fails to claim the digital forensic result, the requesting party or responsible officer shall be administratively charged for Neglect of Duty.

8. RESPONSIBILITIES

a. DDIDM

1. Supervise the implementation of this Investigative Directive; and

2. Perform other tasks as directed.

[11] Pollo v. Constantino-David, et. al. G. R. No. 181881, October 18, 2011

b. D, ACG

1) Responsible for the effective implementation of this Investigative Directive; and

2) Perform other tasks as directed.

c. RDs, PROs

1) Responsible for the proper dissemination and compliance of this Investigative Directive up to the Police Community Precinct (PCP) level of their respective AOR; and

2) Perform other tasks as directed.

d. D, LS

1) Provide legal support and advice in implementing this Investigative Directive; and

2) Perform other tasks as directed.

9. ADMINISTRATIVE SANCTIONS

The filing of any administrative charge pursuant to NAPOLCOM MC 2016-002 shall proceed against a personnel who commit infractions, either through commission or omission, relative to the guidelines set forth in this Investigative Directive.

10. EFFECTIVITY

This Directive shall take effect 15 days upon the date of signing. All prior issuances inconsistent with this Directive are deemed repealed.

AUGUSTO M MARQUEZ, JR
Police Director

Distribution:

RDs, PROs
D, ACG
D, LS

Copy furnished:

PNP Command Group
D- Staff
Dirs, NSUs