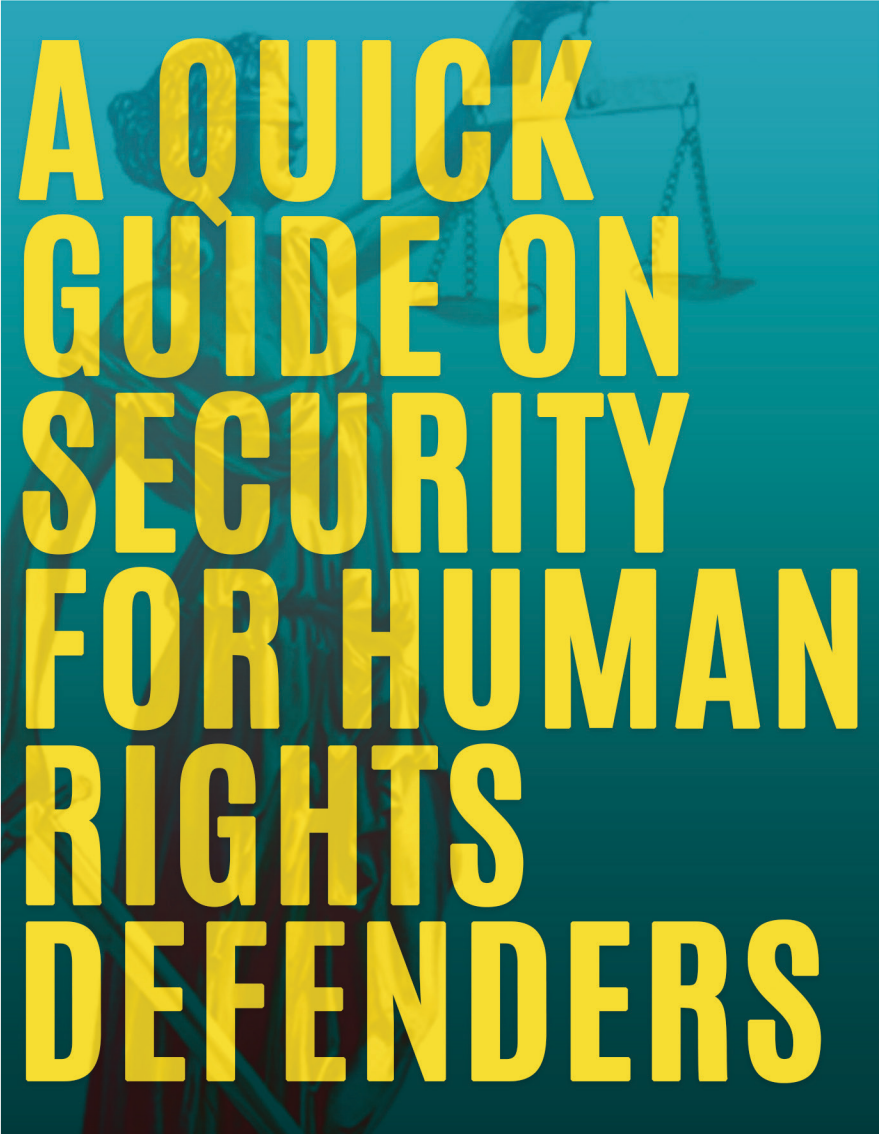


IBON International



A QUICK GUIDE ON SECURITY FOR HUMAN RIGHTS DEFENDERS

A Quick Guide on Security for Human Rights Defenders

CONTENTS

1	Introduction
2	Arrest and Detention
11	Search and Seizures
15	Other Practical Tips
17	Contact Points
18	Emergency Tips & FAQs
21	Information Security
29	Some Suggested Applications

INTRODUCTION

IBON International's core work of solidarity is premised on people-powered democracy. Promotion of people's rights, contributing to developing capacities of organisations entail that we take the extra mile in the conduct of our work. Development workers are human rights defenders in the main.

As human rights defenders, we play an important role in ensuring justice, equality, transparency and accountability in societies. Our legitimate work ensures that peoples' rights and sovereignty are upheld and defended especially in the face of growing corporate greed and government corruption and abuse.

Our work as human rights defenders has always been accompanied with risks to life, liberty and security. Such risks are amplified by the current global trend of closing spaces for peoples' movements and civil society. In the Philippines, the militarist Duterte government has been decisively and brazenly shutting down civic and democratic spaces in its attacks against workers, farmers, the urban poor, Indigenous Peoples, and other toiling people asserting their rights and sovereignty. It is criminalizing dissent and rolling back democratic institutions and checks on Duterte's power as he imposes de facto martial rule and state terrorism in the country. Impunity reigns as domestic mechanisms for supposed accountability are either failing or proven inadequate.

While many human rights defenders understand and internalise the nature of our work, there are many practical tools available to help keep us safer and manage these risks. This handbook is intended as a quick reference for suggestions and steps to improve your personal and digital security situation.

The so-called Anti-Terrorism Act of 2020 (ATA 2020), and the greater use of digital platforms since the novel Coronavirus (COVID-19) pandemic, have increased the physical and information security risks for rights defenders. These warranted updates on the sections of this handbook.

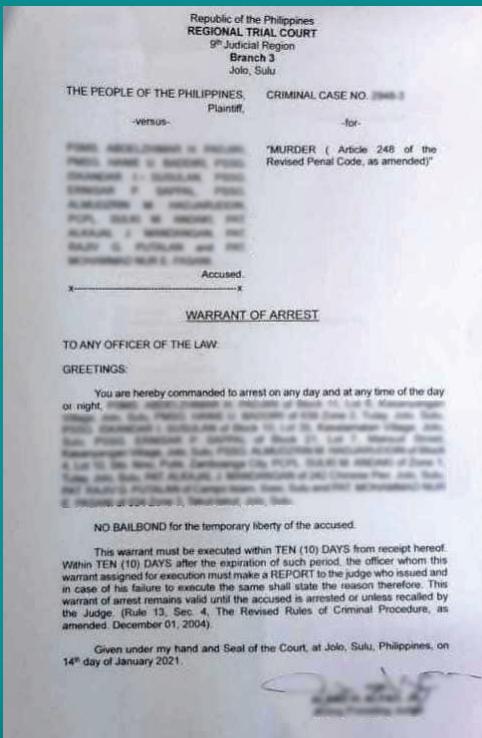
IBON International believes that human rights defenders are critical to achieving genuine progressive, equitable, and sustainable development. We hope that this handbook may help you continue your work for the protection and enhancement of peoples' rights and welfare.

ARREST & DETENTION

What is a warrant of arrest?

A warrant of arrest is a legal document issued by a court and served by a law enforcement officer directing the arrest of a person/s who is/are alleged to have violated the law.

A warrant of arrest issued by Branch 3 of the Jolo Regional Trial Court against respondents to a murder case



How is a warrant of arrest issued?

In the Philippines, a warrant of arrest is not directly applied or issued by the courts.

Cases which carry a penalty of **4 years, 2 months and 1 day imprisonment** as provided for in the Revised Penal Code or Special Laws, shall first undergo a

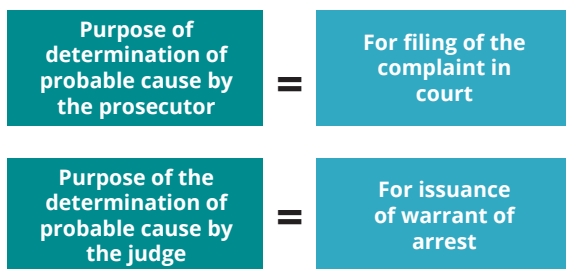
process called **preliminary investigation**.¹ However, in Manila and chartered cities, all cases **regardless of imposable period of imprisonment** shall undergo preliminary investigation, unless otherwise provided in their charters.²

A preliminary investigation is a process where the investigating prosecutor determines whether or not there is probable cause that a crime is committed and the respondent should be held for trial in court. The prosecutor evaluates the pieces of evidence cited by both parties. This process is meant to unclog the courts with cases hastily filed without basis. If the investigating prosecutor finds probable cause, s/he will issue a resolution and information recommending the filing of the case in court. Otherwise, s/he will dismiss the complaint filed.

When is the complaint filed directly in courts?

A complaint is directly filed with the Municipal Trial Courts if the penalty imposed is below 4 years, 2 months and 1 day imprisonment (*except as mentioned above when the complaint is filed in Manila and chartered cities, where preliminary investigation is required in all cases regardless of the imposable penalty*). This means that the preliminary investigation will be conducted by the judge or the prosecutor.³

In any case, if the prosecutor recommends the filing of the case, it will be raffled to the court who will issue the warrant of arrest. The judge where the case was raffled will have its own determination of probable cause, which is separate and independent from the probable cause determined by the prosecutor during the preliminary investigation.⁴



Preliminary Investigation process and issuance of warrant of arrest:

1. Filing of complaint
2. Filing of counter-affidavit by the respondent
3. Filing of reply-affidavit by the complainant

¹ Rule 110, Section 1 (a), The Revised Rules of Criminal Procedure

² Rule 110, Section 1 (b), The Revised Rules of Criminal Procedure

³ Rule 112, Section 6 (b), The Revised Rules of Criminal Procedure

⁴ Rule 112, Section 6, The Revised Rules of Criminal Procedure

4. Filing of rejoinder-affidavit by the respondent – The prosecutor may require clarificatory hearings or require submission of memorandum.
5. Prosecutor decides whether or not to file the case in court – If s/he decides to file it, the prosecutor will prepare and submit a resolution and information in court.
6. Within 10 days from the filing of information, the judge where the case is raffled will personally evaluate the resolution of the prosecutor and examine under oath or affirmation the complainant and its witnesses. S/he will decide if a warrant of arrest will be issued. Otherwise, s/he will dismiss the complaint if it clearly failed to establish probable cause.⁵



What happens if any of the parties fail to file the necessary answer during the preliminary investigation?

The prosecutor will decide based on the documents s/he has on hand.

How long does the prosecutor decide on the case?

According to the Revised Rules of Criminal Procedure,⁶ the investigating prosecutor shall determine whether or not there is sufficient ground to hold the respondent for trial within 10 days after the investigation. However, this is not a hard and fast rule, as in some cases, the resolution of the cases by the prosecutor takes more than 10 days depending on the nature of the case and the workload of the prosecutor and other grounded and reasonable circumstances.

Other facts you need to know about a warrant of arrest:

- The warrant of arrest should be executed 10 days from its receipt by the head of office to whom it was delivered. If not served, the officer will return it to the court and give the reasons why the warrant was not served.⁷ An alias warrant may be issued if the original warrant was not served within the prescribed period.

⁵Section 2, Article III, 1987 Philippine Constitution: “the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.”

⁶Sec. 3 (f) Rule 112, Revised Rules of Criminal Procedure

⁷Section 4 Rule 113, Revised Rules of Criminal Procedure

- Failure to serve the warrant does not dismiss the case. It is still valid and existing and is only archived. It will be revived as soon as the accused is apprehended and brought to court.
- A warrant of arrest should contain the complete and correct spelling of the name of the accused. The warrant should also indicate the court and the name and signature of the judge who issued it.
- The warrant should only indicate one offense, otherwise, it is invalid.

What is a warrantless arrest and when can it be made?

Generally, the law requires that there must be a warrant of arrest issued by a court before a person can be arrested. But the law takes exception in certain instances where the arresting officer and even private citizens may apprehend a person without the need of going through the filing of complaint and preliminary investigation. The reason for this is the urgency of taking a person into custody in the following circumstances:⁸

- When the person to be arrested has committed, is actually committing, or is attempting to commit an offense in the presence of a law enforcement officer or any private person
- When an offense has just been committed and the arresting officer or any private person has probable cause to believe that the person to be arrested has committed a crime
- When the person to be arrested is a prisoner who has:
 - escaped from prison, or the place where he is serving final judgment or is temporarily confined while the case is pending, or
 - escaped while being transferred from one confinement to another.

Anti-Terrorism Act (ATA) of 2020 and the heightened risks of arrests

The ATA gives the power to police and military personnel to conduct arrests without warrant even for persons suspected of the various acts related to “terrorism” -- all are punishable between 12 years to lifetime imprisonment without options for early release. The ATA expands legal reasons for arrests as its definitions are vague and overbroad:⁹

- The notion of “terrorism” now covers crimes already punishable by previous laws such as those acts causing death and injury, or destruction of property.
- Advocacy, protest, dissent, stoppage of work, industrial or mass action, creative, artistic, and cultural expressions, or other similar exercises of civil and political rights can be tagged as terrorism and criminalised on the ground of mere suspicion.

⁸Section 5, Rule 113, Revised Rules of Criminal Procedure

⁹Section 4, Republic Act 11479

- The definition covers “terrorism” in all its “stage[s] of execution”. These include:
 - threat to commit;
 - planning, training, preparing, facilitating (possessing connected objects, documents);
 - conspiracy (agreement between 2 or more persons to “commit terrorism”)
 - proposing;
 - inciting (speeches, writings, proclamations, banners, and other representations);
 - recruitment (including advertisement or propaganda for recruitment, voluntary membership);
 - providing material support.
- These apply to any person who, “within or outside the Philippines,” are considered to have committed such acts.

The Implementing Rules of the ATA gives the Anti-Terror Council (ATC) unbridled authority to start the process of proscribing an individual or organisation as terrorist/s, after which the Justice Department will file an application to proscribe these organizations and individuals in courts. The Court of Appeals could issue a “preliminary order” within 3 days to legally outlaw an organisation or individual, and thus fully, legally subject to arrest. The Anti-Terror Council in itself could also designate organisations and individuals as “terrorists” to freeze their assets.

What is the procedure for warrantless arrest?

In cases of arrests with warrant, the investigation comes first before the issuance of the warrant by the court (via a Preliminary Investigation).

In cases of warrantless arrests, the arrest of a person comes first before the investigation. The arrested individual shall undergo a process called Inquest Proceedings. It is akin to a Preliminary Investigation where probable cause is determined by the investigating prosecutor, who later on decides if the case will be filed in court and hold the respondent for trial.

Under Article 125 of the Revised Penal Code, arresting officers shall only be allowed to hold a person without charges for the following periods:

- 12 hours, for light offenses punishable by light penalties (ex. Unjust vexation and violation of local ordinance).
- 18 hours, for less grave offenses punishable by correctional penalties (ex. Illegal assembly).
- 36 hours, for grave offenses punishable by capital penalties (ex. Murder, arson, kidnapping).

Failure to charge a person in the above mentioned periods in court shall make the public officer and employee liable for violation of Article 125 and arbitrary detention, without prejudice to the filing of other civil and administrative charges, except if it is grounded on reasonable delays.

Note: In applying the provision regarding the period of detention, *there must already be an information filed in court*, and not merely a complaint filed with the Office of the Prosecutor. This means that the investigating prosecutor *already found probable cause* to hold the accused for trial.

How is the legal period of detention affected by the Anti-Terrorism Act of 2020?

The above period of detention is completely disregarded under the Anti-Terrorism Act of 2020. From the usual 36 hours under the Revised Rules on Criminal Procedure, it is prolonged to 14-24 days of detention without charges:

- Under the ATA 2020, persons “suspected of committing” acts under the law’s definition of terrorism could be detained for 14 days which may be extended up to 10 days more.¹⁰
- In cases where evidence of guilt is strong, the court, upon the application of the prosecutor, may limit the right of travel of the accused within the municipality where s/he resides or where the case is pending. S/he may also be placed under house arrest and may not use telephones, cellphones, e-mail, computer, the internet or other means of communication with people outside the residence unless otherwise ordered by the court.¹¹
- The Anti-Money Laundering Council (AMLC) also has the authority to investigate, inquire into and examine bank deposits.¹²
- The AMLC upon its own initiative or upon the request of the ATC is authorized to issue an *ex-parte* order to freeze without delay.¹³

What happens after a person is arrested without a warrant?

- The arrested person should be immediately brought to the nearest police station and undergo a booking process which includes taking of mugshot photos as well as fingerprints. S/he will also be taken to a hospital for a physical examination.
- The arrested individual will be brought to the investigating prosecutor for inquest who will determine if there is probable cause based on the complaint filed by the arresting officer and the evidence s/he produced.
- Counsel for the accused is required to be present during inquest. S/he may engage the services of a private lawyer or if s/he is not able to find one, s/he

¹⁰ Section 29, Republic Act 11479

¹¹ Section 33, Republic Act 11479

¹² Section 35, Republic Act 11479

¹³ Section 36, Republic Act 11479

will be assisted by a lawyer from the Public Attorney's Office (PAO).

- The arrested person will be asked if s/he is willing to waive Article 125 of the Revised Penal Code. If the respondent will waive Article 125, the inquest proceedings will not proceed. This means that the case will undergo the regular preliminary investigation instead, and parties shall exchange affidavits to answer their respective allegations. If the respondent will not waive Article 125, the inquest proceedings will proceed and the investigating prosecutor usually decides on the basis of the complaint filed by the complainant/arresting officers. The respondent will not be afforded a chance to file a counter-affidavit as it is only available during preliminary investigation. Therefore, if s/he wishes to file a counter-affidavit, it is necessary to waive Article 125.

Note: If the inquest proceeding is concluded, the investigating prosecutor may issue any of the following:

- Recommend the filing of the case in court
- Dismiss the complaint and order the release of the respondent from detention unless s/he is being detained for some other lawful grounds
- Recommend the case for further investigation and order the release of the respondent from detention unless s/he is being detained for some other lawful ground. This means that the prosecutor finds the evidence against the respondent to be insufficient and will require the parties to undergo the regular preliminary investigation to answer the allegations through exchange of affidavits.

Things to remember if arrested *with or without a warrant*:

- The arresting officer must inform the person being arrested of the reason for the arrest and apprise him/her of his/her right to remain silent and right to counsel of choice (Miranda Rights).
- The person arrested should be brought to the nearest police station and not in a military camp, safe house or other similar places of detention and must not be placed in solitary confinement.
- Any form of torture (physical, mental or psychological) is prohibited by law under the Anti-Torture Act.
- The arrested person has the right to call and be visited by his/her relatives, a doctor, priest and a lawyer.
- The arrested individual cannot be forced to sign anything. If forced, intimidated or harassed to do so, s/he can put the initials "UP" (Under Pressure) or "UD" (Under Duress) in his/her signature that indicates that he/she did not voluntarily sign any document.
- The arrested person should not be subjected to custodial investigation or questioning without the presence of a lawyer of his/her choice. Any testimony

or evidence obtained during such investigation will be inadmissible in any court or tribunal.

- Lawyer-client privileged communication must be respected at all times. Officers cannot eavesdrop nor stay within hearing distance of the accused and his/her lawyer.

What to do when arrested:

- Stay calm and do not panic so you can think of ways on how to deal with the situation.
- Immediately inform your friends, colleagues, family members, etc., through the phone about your situation.
- Demand for a warrant of arrest and carefully scrutinize the contents.
- In case of a warrantless arrest, the arresting officer must state the reason for the arrest and recite the Miranda Rights.
- If forcibly arrested or raided in the house or office, immediately make a scene to attract public attention by informing any bystander or witness to the incident of your name and other relevant information. You can also use your smart phone and social media to publicize and document the incident.
- Take note of the name/rank, number of arresting officers or physical description such as height, weight, complexion or identifying marks, and plate number of the vehicle used.
- If threatened with arrest while outside the residence/office, immediately empty your bag in public to show that you do not possess any firearm or explosive or illegal items and to avoid the opportunity for authorities to plant evidence in your belongings.
- Do not sign anything without the presence of a lawyer of your choice.
- Demand that you need to call any of your relatives, lawyer, doctor, priest, pastor or human rights organisation/s, etc.
- You can refuse to accept the services of any lawyer provided by the police or military.
- You can refuse to have your picture taken, be fingerprinted, be subjected to bodily search, or do any act which may incriminate you (i.e., physical examination) until you have appointed your chosen lawyer.

What is bail?

Bail is the security given for the release of a person in custody of the law, furnished by him or a bondsman, to guarantee his appearance before any court as required under the conditions specified under the Rules of Court.¹⁴

¹⁴Section 1, Rule 114, Revised Rules of Criminal Procedure

Who may post bail?

All persons in custody shall be admitted to bail **as a matter of right before or after conviction** by the Metropolitan Trial Court, Municipal Trial Court and Municipal Circuit Trial Court.

However **in cases filed with the Regional Trial Courts, bail as a matter of right is only available before conviction if the offense is not punishable by reclusion perpetua** (which ranges from 20 years and 1 day to 30 years in prison) or any crime covered by special laws with the penalty of life imprisonment.¹⁵

If the alleged crime committed is punishable by reclusion perpetua or life imprisonment, the accused will not be allowed to post bail without the permission and approval of the court. In this case, s/he will need to file a **petition for bail** first. The court will conduct a bail hearing. If the evidence of guilt is strong, the court will not allow the accused to post bail.

Bail ensures the court that the accused who posted bail will appear before it whenever required. If s/he fails to do so despite notice, he will be rearrested and the court may issue a bench warrant. The bail will also be forfeited.

Note: Bail is paid and filed only to the court and never to the police/military or any person.

There are four types of bail:

- Cash bond¹⁶
- Property bond¹⁷
- Corporate bond¹⁸
- Recognizance¹⁹

Bail and the ATA

Under the ATA, if the evidence of guilt is not strong, and the person charged is entitled to and granted bail, the court upon application by the prosecutor shall limit the right to travel of the accused to within the municipality or city where s/he resides or where the case is pending, in the interest of national security and public safety. The Court shall immediately furnish the DOJ and the Bureau of Immigration with the copy of the said order. Travel outside of said municipality or city without authorization of the court shall be deemed a violation of the terms and conditions of his/her bail, which shall be forfeited under the Rules of Court.²⁰

¹⁵ Sections 4 and 5, Rule 114, Revised Rules of Criminal Procedure

¹⁶ Section 14, Rule 114, Revised Rules on Criminal Procedure

¹⁷ Section 11, Rule 114, Revised Rules on Criminal Procedure

¹⁸ Section 10, Rule 114, Revised Rules on Criminal Procedure

¹⁹ Section 15, Rule 114 Revised Rules on Criminal Procedure

²⁰ Sec. 34, paragraph 3, RA 11479

SEARCH & SEIZURE

What is a search warrant?

A search warrant is an order in writing issued in the name of the People of the Philippines, signed by a judge and directed to a peace officer, commanding him to search for personal property described therein and bring it before the court.²¹

Search warrant for guns and ammunition issued by Branch 21 of the Northern Samar Regional Trial Court

Republic of the Philippines
REGIONAL TRIAL COURT
8th Judicial Region
Branch 21
Laoang, Northern Samar

Republic of the Philippines,
Complainant,

versus

SEARCH WARRANT No. 07
For: Vio. of Sec. 28, RA 10591

Respondent.

SEARCH WARRANT

TO ANY OFFICER OF THE LAW:

Greetings:

You are hereby ordered to SEARCH and SEIZE the following items which is under the control/possession of respondent _____ of Brgy. San Roque, San Isidro, Northern Samar, to wit:

- One (1) Cal. Pistol of unknown models with several live ammunitions of said firearms;
- One (1) Cal. 9mm pistol of unknown models with several live ammunitions of said firearms.

to be guided by the location map as well as the residential house sketch as attached in the application for search warrant indicating the particular place and location of the items to be search and seize.

The Officer is hereby enjoined to observed Section 11 of Rule 126 of the Rules of Court as well as Section 12 thereof, which is delivery of property and inventory thereof to this Court.

In Chambers, Laoang, Northern Samar, this 3rd day of October 2016.

Executive Judge

What are the requirements for issuing a search warrant?²²

The Revised Rules of Criminal Procedure provides requirements for issuing search warrants. Remember that any evidence obtained in violation of the requirements (below) is inadmissible for any purpose in any proceeding.

²¹ Section 1, Rule 126, Revised Rules of Criminal Procedure

²² Sections 4,5 and 6, Rule 126, Revised Rules of Criminal Procedure

Section 4- *Requisites for issuing a search warrant.* — “A search warrant shall not be issued except upon probable cause in connection with one specific offense to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the things to be seized which may be anywhere in the Philippines.”

Section 5- *Examination of complainant; record.* — “The judge must, before issuing the warrant, personally examine in the form of searching questions and answers, in writing and under oath, the complainant and the witnesses he may produce on facts personally known to them and attach to the record their sworn statements, together with the affidavits submitted.

Section 6- *Issuance and form of search warrant.* — “If the judge is satisfied of the existence of facts upon which the application is based or that there is probable cause to believe that they exist, he shall issue the warrant, which must be substantially in the form prescribed by the Rules.”

Where should one file an application for search warrant?²³

- Any court within the territorial jurisdiction of the crime
- For compelling reasons stated in the application, any court within judicial region where the crime was committed or where the warrant shall be enforced. However, if the criminal action has already been filed, the application shall only be made in the court where the criminal action is pending.

Note: There are exemptions to the requirement that a compelling reason must be stated in the application for Search Warrant if applied outside the place where it will be served.²⁴ Executive Judges or in their absence, the Vice-executive Judges of Regional Trial Courts of Manila and Quezon City, can issue search warrant that can be served anywhere in the Philippines as long as the application will be endorsed by Chief of Office of PNP units. This has been used in cases in Negros, Central Philippines, where the Search Warrants were applied and issued in Quezon City but enforced outside Metro Manila.

These special criminal cases involve the following charges:

- Heinous crimes
- Illegal gambling
- Illegal possession of firearms and ammunitions
- Violations of the Anti-dangerous drugs law, the intellectual property code, the Anti-money Laundering Act, the Tariff and Customs Code, and other relevant laws that may be enacted by Congress and may be included in the law by the Supreme Court.

²³ Section 2, Rule 126, Rules of Court

²⁴ AM. No. 99-20-09-SC (Resolution Clarifying Guidelines on the Application for and Enforceability of Search Warrants)

When should the search warrant be executed?

The warrant must direct that it be served in the day time, unless the affidavit asserts that the property is on the person or in the place ordered to be searched, in which case a direction may be inserted that it be served at any time of the day or night.²⁵

Until when is the search warrant valid?

A search warrant shall be valid for ten (10) days from its date. After this period, it shall be void.²⁶

In what instances would a search and seizure without warrant be allowed?

- A warrantless search incidental to a lawful arrest²⁷
- Search of evidence in plain view, or with evidence immediately visible
- Search of a moving vehicle
- Consented warrantless searches
- Customs searches
- Stop and frisk
- Exigent and emergency circumstances
- Checkpoints
- Republic Act requiring inspections or body checks in airports
- State of Emergency
- In times of war and within military operations

What is plain view?

In criminal law, the plain view doctrine allows a law enforcer to make a search and seizure without obtaining a search warrant if the evidence of criminal activity or the product of a crime can be seen without further search.

The plain view doctrine states that objects in the plain view of an officer who has the right to be in the position to have that view are subject to seizure without search warrant and may be presented in evidence. The doctrine cannot be used to launch unbridled searches and indiscriminate seizures nor to extend a general exploratory search made solely to find evidence of the accused's guilt. It is applied where a peace officer is not searching for evidence or that he has prior justification for an intrusion, in the course of which he came inadvertently across a piece of evidence incriminating the accused, and permits the warrantless seizure thereof.²⁸

²⁵ Section 9, Rule 126, Rules of Court

²⁶ Section 10, Rule 126, Rules of Court

²⁷ Section 13, Rule 126, Rules of Court

²⁸ Agpalo, R. E. (1997). p. 539, Agpalo's Legal Words and Phrases (1997 ed.). Rex Bookstore, citing the case of *People v. Musa*, 217 SCRA 597 [1993].

When can evidence be seized in plain view?

- Searching officer must be in a place s/he has a right to be in.
- Discovery of the evidence must be inadvertent.
- The seized evidence must be immediately apparent without further search. The person arrested should be brought to the nearest police station and not in a military camp, safe house or other similar places of detention and must not be placed in solitary confinement.

Important things to remember in case of search and seizure

- Always demand for a search warrant and scrutinize it. **Search warrants must contain the correct and complete address of the premises being searched.**
- Search warrant must pertain to a single offense. Therefore if the allegation is for possession of firearms and explosives, there must be two (2) separate search warrants as it pertains to separate offenses.
- No search of a house, room, or any other premises shall be made except in the presence of the **lawful occupant or any member of his/ her family or two witnesses of legal age and residing in the same locality.**²⁹
- **The following are the only personal property to be seized:**³⁰
 - (a) Subject of the offense;
 - (b) Stolen or embezzled and other proceeds, or fruits of the offense; or
 - (c) Used or intended to be used as the means of committing an offense.
- The officer must give a detailed receipt to the lawful occupant of the premises who was a witness to the search and seizure. In the absence of the occupant, the receipt must be left in the presence of at least 2 witnesses of legal age in the place in which the seized property was found.³¹
- The owner of the things seized cannot be forced to sign the receipt of the items seized.

²⁹ Section 8, Rule 126, Rules of Court

³⁰ Section 3, Rule 126, Rules of Court

³¹ Section 11, Rule 126, Rules of Court

STAGES OF TRIAL

- A. Arraignment and pre-trial
- B. Presentation of prosecution evidence
- C. Presentation of defense evidence
- D. Judgment
- E. Appeal
- F. Execution

Under the ATA 2020, the newly-formed Anti-Terrorism Council is mandated to “request” the Supreme Court to designate specific divisions of the Court of Appeals and Regional Trial Courts as “anti-terror courts” for the trial of all persons charged under the new law.

OTHER PRACTICAL TIPS

- If you think that your life/security is in danger, consult with your organisation.
- During an arrest or search, keep calm but stay alert and assess the situation.
- In case of an imminent or an ongoing search, take a video of your surroundings for documentation purposes.
- Practice to know and remember details (plate number, color of car, description of faces).
- Keep contacts of lawyers, friends, or family who can immediately respond to your situation.
- Think of how to get out of the situation you are in without compromising your safety.
- Make good judgments based on the concrete situation.

Travel Documents and Essentials

- Approved travel authorization
- Travel documents
 - Passport and Visa*
 - Plane tickets*
 - Employment Certificate*
 - Logistics note*

- Insurance*
- Accommodation*
- Invitation Letter*
- Country briefer
- Others
 - Money
 - Travel adapter and phone

**Print three copies for self, family, and office.*

When in an overseas trip, especially when staying and traveling in crowded cities, be very vigilant and careful of your belongings. Do not simply accept unsolicited offers of “help” from strangers.

If you become a victim of theft:

- File a report at the nearest police station.
- Contact your office.
- If your passport has been stolen, contact your embassy consulate for issuance of temporary travel documents.

CONTACT POINTS

	Name	Phone	Email	Address
Organisation				
Local Host				
Family				
Insurance				
Embassy				

Organisation

Each organisation is highly encouraged to designate a Quick Response Team (QRT) and referral pathways for emergencies that may be encountered by staff on official duty travel (ODT) abroad. Establish policies and procedures on ODT and emergencies abroad, inform all staff of these, and ensure that all travelling staff know the contact details of the QRT. Each organisation should have a system to ensure that all travelling staff are monitored.

Local Host

Most of our travels are by invitation and coordinated by a local host. Otherwise, it is highly suggested for your organisation to endorse you to a network or allied contacts

Family

Inform your family ahead on the nature of our work and the risks we face abroad. Give the basic details of your travel including itinerary, inviting group and activity. Decide which family member will be the contact in case of emergency and establish communication lines with your organisation.

EMERGENCY TIPS & FAQs

Every country has its own laws and procedures. The legal system in your destination country may be very different from the one at home. Getting support from your organisation and local host as quickly as possible is important.

Use an interpreter

Do not rely on your knowledge of the foreign language unless you are completely fluent. Ask for a professional and independent interpreter you trust. Do not take legal advice from interpreters or let them influence the way your case progresses.

What information should I share with State officers?

- Demand to speak to a lawyer of your choice. Assert your right to remain silent. Everything you say may be used against you, so think before you speak.
- Do not offer unnecessary and excessive information.
- Make sure you understand everything. Officers may coax you into revealing private and confidential information. For legal cases, always confirm with your lawyer before you say anything.

Should I sign documents?

- Never sign blank pages. Never sign a document written in a language you do not fully understand.
- Ask for a written translation of all documents and sign only the translated copy which you fully understand.
- If there is no written translation, ask for your interpreter to translate verbally before you sign a document. Make sure you write next to your signature that you did not understand the content of the document.

I was held at the airport. What should I do?

- If you are held at the local airport, contact your organization immediately. As soon as you land in your destination, report to your organisation and local host. In case of any delay, they will know that your last contact is at the airport.
- Respond to questions by immigration officers and airport officials in a cordial manner and present travel documents as necessary. If you are being held, ask them why, if permissible.
- In most countries, you are not entitled to an attorney during primary and secondary inspection at the airport. Keep your contact points handy and inform them if you feel your rights are being violated or if you have been

detained for an unusually long period. Alert your local host immediately.

- Each country has varied reasons for denying entry to a foreigner. In case you will be deported, ask them why, if permissible.

I have been held in custody and/or arrested abroad. What should I do?

1. Know your rights.

- Ask custodial/arresting officers to explain or provide a written statement of your rights in a language you understand, when permissible.
- In case of arrest, remember the Miranda Rights that an arresting officer normally says:
 - You have the right to remain silent.
 - Anything you say can and will be used against you in a court of law.
 - You have the right to an attorney. If you cannot afford one, the State will provide for you.
 - Do you understand the rights I have just read to you?
 - With these rights in mind, do you wish to speak to me?
- Ask questions to clarify your rights, when necessary and permissible. The Miranda doctrine is not a universal law but there are equivalent rights in other countries. Here are some guide questions you can ask:
 - **Do I have a right to remain silent?** Could my silence be used against me?
 - **Do I have a right to a lawyer?** Will the state provide me and pay for this lawyer? When can I see my lawyer?
 - **Do I have a right to an interpreter?** Will the state provide me and pay for this interpreter? Is there a translation of written documents in English or a language I understand?
 - **Is the investigation complete?** If not, when will it be completed? Who is doing the investigation?
 - **How long can I be held in custody?** If there is no case, when will I be released?
 - **If there is a case, when will I be taken to a fiscal/judge?** When will the trial begin? Can I apply for bail? If yes, when?

2. Notify your organisation, local host, and family.

Share important details:

- Date and place of arrest;
- Where you are being detained, including prisoner number;
- Names of arresting officers, if possible;
- Reason for your arrest and charges against you;
- Important dates and time-limits in your case;
- Lawyer's name and contact details, if you have one already;
- Consular representative's name and contact.

In case you cannot contact them directly, pass the information on to someone you can trust to forward to your family. This may sometimes include the prison social worker, consular representative or your lawyer.

3. Seek legal advice and services from a lawyer who is qualified to practice in the jurisdiction you are in.

- Your organisation should ensure securing a lawyer for you.
- Your local host or embassy may be able to provide you with a list of local lawyers who speak your language.
- Do not be rushed into appointing a specific lawyer on the advice of anyone with a vested interest in the case.
- Maximize time at the first instance, do not wait for the next meeting with your lawyer. Prepare by writing questions ahead and take notes of discussions. Give all the information that will help with your defense including pieces of evidence and witnesses. And ask what will make your case stronger.

4. Be wary of fellow prisoners/detainees.

Do not share information about your case with fellow prisoners/detainees or rely on any legal advice they give you.

5. Request for a consular representative to visit you.

- Ask your custodial/prison officer or your consulate to arrange a private visit, if permissible.
- Make sure you inform him/her of any mistreatment, document your injuries, and request to see a doctor. Keep as much evidence.
- Report other welfare issues and inform them of any medical conditions or medicines you need.
- Request them to inform your contact points (organisation, local host, family, lawyer) to update about your situation and needs.

REMINDERS:

Be calm.

Know your rights.

Get information about your case.

Notify your contact points.

INFORMATION SECURITY

Why is information security needed?

A non-governmental organisation/people's organisation and its staff/members receive, process and share information about its work on a daily basis. Your organisation and its staff/ members need to secure vital information about your work from possible threats of unwanted distribution to, and breach by repressive state actors and malicious private individuals.

Depending on the situation, carelessness on information security might create risks for individuals or for the whole organisation itself. This is especially important with laws such as the ATA of 2020, which expands surveillance allowed under law.

Expanded surveillance under ATA 2020

The ATA 2020 expands permissible surveillance even of persons only suspected to fall under the overbroad definition of "terrorism." Police and military personnel "may secretly wiretap, overhear and listen to, intercept, screen, read, surveil, record or collect" their private communications and information through all possible means "known to science." The only supposed exceptions are information between lawyers and clients, doctors and patients, journalists and their sources, and business information.

Police and military personnel, through just a Court of Appeals order, may compel telecommunications companies and internet service companies to "produce all relevant customer information," including identification, call and text data records, and other cellular and internet metadata, of the same suspected persons. Companies have to comply within 48 hours.

What information needs to be protected?

- Identify which among your files and information are for public use (e.g., finished research papers) and which are considered private, confidential, and sensitive.
- Information considered private, confidential, or sensitive must be accessed and distributed only within the organisation.
- Known when it is necessary to limit access to certain sensitive information within certain members of the organisation (e.g. management/officers).

How do you secure your information as an organisation?

- Keep physical documents safe. This should respond to possible risks such as physical damage, theft, accidental loss, and other emergencies.
- Exercise care in limiting, or in some cases preventing, dissemination of private, confidential, and sensitive files and information through online channels. Connecting online allows you to reach other organisations, but also makes it possible to get your information.

How can your organisation improve the physical storage and security of information?

- There must be systems to handle organisational documents and files.
- The organisation should have administrative personnel whose primary tasks are handling and keeping such documents. Still, all of the organisation's members handle different kinds of information about daily operations and are all responsible for keeping these accessible only to the necessary people.
- Formulate and implement security protocols and policies on storing, handling, and accessing information to prevent unwanted breach. This includes: creating secure back-ups of essential organisational files, protocols on securing files in case of emergencies, and controlling access to your office premises and information storage. For example, keep track of the visitors who enter office premises (e.g., through logbooks) and limiting their physical access to certain areas if necessary.
- Put in place physical infrastructure adequate to security needs, from sturdy, secure, fire- and waterproof containers for files (e.g., with sturdier containers for more sensitive files), quality locks on office doors and gates, wired security cameras especially on strategic areas of offices (e.g., location of finance files, entrances, exits), with the location of the drives storing security footage known only to relevant personnel.

What if people ask me about personal but private information?

Networking and advocacy require conversations about your work, and about certain people within your organisation. But you have the right to kindly refuse giving private details about individuals from your organisation. For example, if you are asked by an unidentified individual, especially through a call/email, about personal information such as personal addresses or private phone numbers, you should not give these to the said unknown person/unverified entity. Secondly, identify who is seeking the information.

Public	Private	Confidential	Behavioral	Sensitive
Full name	Civil status	Previous employer	Favourite food	Photo of children or pets
Birthday	Age	Elementary school	Photo at a social event	Photo of your house
Current employer	Personal email address	High school	Favourite movies	Mother's maiden name
Current job designation	Personal contact no.	Year graduated from college	Favourite hangouts	First pet
Work email address	Photo with family	Years in current office	Favourite music	Location of hometown
Photo of yourself	Photo with friends	Place of birth	Photos while doing hobbies	Photo of ID

How can your organisation enhance online and device security?

- Assign **staff/members of the organisation** primarily tasked to handle information technology concerns, including digital security. All staff/ members must be aware of secure online habits, and practice them (see next section).
- Formulate and implement **security protocols and policies** for office devices and internet access and use, including for online browsing, e-mails, grouplists, cloud storage services (e.g., Google Drive), social media and other communications channels.
- Put in place **appropriate infrastructure**, such as firewalls for the organisation's servers and website/s. Ensure maintenance of computers and office devices that connect online.

What general measures could you take as an organization to safeguard devices and internet connections?

Depending on the organisation and situation, measures include but are not limited to:

- Securing files - Protect confidential and sensitive files with passphrases.
- Internet connections - Have secure passphrases on office internet/WiFi

connections. To minimize risks, limit computers that work on confidential files (e.g., finances) from connecting online.

- Blocked websites - Set risky websites to be blocked, prevent unnecessary online traffic.
- Cloud services - Limit the use of cloud services for storing sensitive organisational files.
- Organisational accounts - Regularly change passwords for the organisation's social media channels, e-mails.
- Platforms that track your data - Move away from platforms that heavily track user information (e.g., Google platforms such as Gmail, Google Drive, and others).
- Online calls and meetings - Add room passwords, or use registration links, if there is a need to limit the online attendance to certain persons. In certain instances, it would be important to have a way of verifying the identities of fellow participants in a call.

How can you ensure the physical security of your workplace?

- Be conscious that nobody has unwanted access to the devices you use at work, and if applicable, your workspace.
- Be careful to not leave your work or even personal devices unlocked at your desks/workspaces.
- Refrain from leaving your devices unattended in public places.
- These are in addition to practicing the measures your organisation has established.

What are the dos and don'ts to enhance the security of your devices, including mobile devices?

Anti-viruses and anti-malware.

- Install, and regularly update, anti-virus and anti-malware software on your computers, such as Avast and Malwarebytes. These applications can block malicious files from infecting your computer.
- Remember to scan your computers regularly with your anti-virus and anti-malware applications.

Computer settings

- Adjust your computer settings to limit the information being shared to companies or whoever might be trying to access your devices. In your Settings/System Preferences, ensure the following:
 - Location – “Allow access to location on this device” to “Off”
 - Microphone – “Allow access to the microphone” to “Off”
 - Camera – “Allow apps to access your camera” to “Off”

Secure passphrases

- Use passphrases more than passwords, as password-cracking applications used by malicious individuals will find longer phrases more difficult.
- Choose passphrases that are familiar enough to you but not predictable for other people.
- Combine uppercase and lowercase letters, numbers and special characters to increase password difficulty.
- Have different passphrases or passwords for different accounts. Never reuse a password. This is applicable to your computers, mobile devices, social media and e-mail accounts, and others.
- Do not save your password, or the “remember my password” option, for your accounts.
- Change passwords regularly, especially if you feel that your accounts have been breached.
- There are also applications you can use to keep different passphrases and passwords, such as KeePass (see “Some suggested applications” box below).

Keeping files.

- Classify the information stored in your computers and devices as public, and which is private, confidential, and sensitive.
- Back up those that are vital to your work.
- Don’t leave private, confidential, and sensitive files in your computers and devices easily accessible. If necessary, do encrypt them (see “Other tips related to information security” on how).

Mobile applications.

- In the Application Settings of your phone, turn off “app permissions” that are not necessary, such as permissions to your microphone, location, messages, or contacts. For instance, if it’s a photo application, there is no reason for it to access your messages or your location.

What are the dos and don’ts when connected online?

- Practice online browsing habits that minimize unnecessary and malicious exposure of your information to third parties.
- You may use applications, email clients, and browser add-ons that also help in secure communications and browsing. But, not practicing safe browsing habits despite having good applications still increases threats to your online privacy.

Browsing, searching online:

- Do not click pop-up advertisements or even banner advertisements. In the settings of your browser application, disable saving passwords, be sure to click the options to block pop-ups, and the “do not track” option.

- Refrain from downloading suggestive applications being offered by websites.
- Use “Incognito Window” or “Private Window” options available in your choice of browser. For example, the Firefox incognito window clears your search and browsing history when you quit the browser.
- Move away from platforms known for tracking your browsing to sell it to advertising companies, such as Google. For example, for search engines, you may use more private search sites such as DuckDuckGo, or Mozilla Firefox, or TOR, for browsers (see “Some suggested applications” below).
- In your browser, use add-ons such as Adblock Plus to block ads. Using Privacy Badger is another way to stop third parties from tracking you.

E-mail:

- Be mindful of senders, attachments, and links. Common suspicious e-mails include winning contests you haven’t entered, or instructions to change your bank account passwords online. Refrain from clicking on suspicious emails, or on the links in these e-mails.
- Separate work from personal email accounts. If somebody needs to communicate with you about work concerns, give them your work email account, and for personal concerns give them your private e-mail account.
- You may shift away from Google Mail, as they analyse even your email content to “customize search results” among other purposes. You may use Protonmail instead. Also, use a non-browser based email application, such as Thunderbird.

Social media and instant messaging:

- Refrain from unnecessarily sharing information. This includes passport details, bank account details, and even your location. These also include files from your work that are considered private, confidential and sensitive.
- If information about a trip, event or meeting is not immediately for the public, it is sometimes better to avoid posting photos and details as they happen (e.g., “at the moment” posts).
- In cases where online instant messaging is unavoidable, use applications such as Signal (see “Some suggested applications”). Avoid interlinking your social media accounts (e.g., Facebook) as a user account in other applications.

Using public WiFi/internet connections:

- Anyone can connect to public internet connections, including individuals wanting to spy and get your data.
- If you have no choice but to connect to public WiFi hotspots in airports, cafes, malls, you may want to make your browsing “anonymous” by using a Virtual Private Network (VPN).

Summary: Dos and don'ts for individual devices and browsing

On your computers/mobile devices:

- Do install an anti-virus and an anti-malware on your computers, and remember to scan regularly.
- Do create strong passphrases, and have different ones for your accounts and for your devices.
- Do back up those files vital to your work.
- Do use a camera cover for your devices
- Don't allow unnecessary tracking of your device activity by turning off automatic access to location, camera, and microphone. In mobile, don't allow unnecessary mobile application permissions.
- Don't be careless about private, confidential, and sensitive files; encrypt them if necessary.

On connecting online:

- Do use a VPN, browser applications, and search engines that commit to not tracking your information, especially when using public WiFi in airports, cafes, or malls.
- Do adjust browser settings to prevent others from tracking your internet activity
- Don't use online banking when using public internet connections.
- Don't click pop-ups (and immediately close them if accidentally clicked) and suspicious emails and sites.
- Don't unnecessarily disclose on social media where you are or who you are with.

Checklist: To do's in information security when travelling abroad

- **Preparations:** Make time to check your laptop files and phones when flying out. Ensure that you don't have confidential files with you.
- **Before travelling (from and back to your country):** Maintain secure communication lines for contacting your organisation, and/or partners who will be on standby in case of an emergency.
- **Upon arrival abroad:** Buy a SIM card for a personal internet connection instead of using public WiFi hotspots, especially when in sensitive security situations.
- **While abroad, going abroad:** Follow dos and don'ts in browsing online, such as using a VPN or TOR browser if you have no choice but to connect to public WiFi hotspots, etc.

Other tips related to information security

Backing up files.

Flash drives are the easiest storage device for backing up your files but their portability can also mean they can easily be lost. It is advised that you have at least three back-up files on three storage devices. Protect your storage devices with a password.

Encrypting files.

Encrypting files means securing them in your storage devices, with password protection. Sometimes you may need to encrypt your private, confidential, and sensitive files. You may use applications such as VeraCrypt. If so, do not forget and never share your password to not lose your access to your secured files.

Securely delete files.

Deletion by clearing out your computers' Recycle Bins still leaves some data that can be traced by other parties with the right recovery applications. If the situation demands a more thorough deletion of private, confidential, and sensitive files, you may use applications such as Eraser.

Some suggested applications



Malwarebytes

Malwarebytes

Anti-malware application



KeePass

KeePass

Password storage



ProtonVPN

Free VPN, requires a protonmail account



Signal

Signal

Encrypted messaging



Mozilla Firefox

Browser



Eraser

Secure deletion



TOR

Browser



VeraCrypt

VeraCrypt

File encryption



DuckDuckGo

Duckduckgo.com

Search engine



Jitsi Meet

Jitsi Meet

Online call platform with end-to-end encryption options

References

Karapatan, http://karapatan.org/files/BUST%20CARD%20ENG_TAG%2020170313.pdf

Miranda Rights, <http://www.mirandawarning.org/whatareyourmirandarights.html>

Fair Trials International, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/320911/Annex_8_-_FTI_-_Arrested_in_another_country.pdf

Computer Professionals' Union. 2019. Information Security Training Workshop. Training held at IBON International, Quezon City, Philippines.

Karapatan. 2019. Human Rights and Security Training Workshop. Training held at IBON International, Quezon City, Philippines.

Republic Act No. 11479. "The Anti-Terrorism Act of 2020."

The 2020 Implementing Rules and Regulations of Republic Act No. 11479.

