



*sflc.in*  
**Guide**

# **SEARCH & SEIZURE OF ELECTRONIC DEVICES**

## **Guide on Search and Seizure of Electronic Devices, 2025**

By SFLC.in in partnership with UNESCO

© Copyright 2024 SFLC.in Licensed under Creative Commons BY SA NC 4.0

Published by: SFLC.in

K9, 2nd Floor, Birbal Road, Jangpura Extension, New Delhi – 14, India.

Email: [mail@sflc.in](mailto:mail@sflc.in)

Website: <https://www.sflc.in>



# TABLE OF CONTENTS

<b>01.</b>	Section 1 <b>The Basics</b>	4
<b>02.</b>	Section 2 <b>What to do during a search?</b>	10
<b>03.</b>	Section 3 <b>Electronic Devices and the Law</b>	14
<b>04.</b>	Section 4 <b>Post-Seizure Protocol</b>	16
<b>05.</b>	Section 5 <b>Preparedness</b>	25
●	<b>Glossary</b>	33
●	<b>Annexure</b>	36
●	<b>References</b>	45

**section 1**

# **THE BASICS**



**HAVE YOU BEEN SEARCHED BY ANYONE?**  
**DID THEY SEARCH YOUR BODY, VEHICLE, HOME?**  
**DID THEY SEIZE YOUR DEVICES?**  
**IF THE ANSWER TO ANY OF THESE IS YES...**



# SEARCH & SEIZURE DECODED

## Search and Seizure: What, Why, and Where

**'Search'** means looking into an individual or their property [1] to find evidence for an ongoing investigation or a judicial proceeding [2]. This can be done with [3] or without warrant. [4]

**'Seizure'** means taking possession of that property once the search is done to be used as evidence or as the property concerned for an investigation. [5]

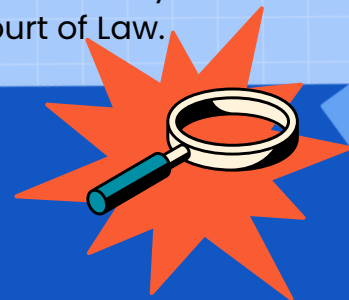
**What:** It is the tool used by law enforcement agencies to investigate a case.

**Why:** It is done to collect evidence, prevent crime, and deter miscarriage of justice.

**Where:** Scenes where the crime was conducted, locations where people involved in the crime may be hiding, and locations where any materials related to the crime may be kept.

## Reasons behind Search & Seizure

- It is done to ensure that crucial objects and documents including electronic and digital records are made available to any agency for investigation, inquiry, or trial against a person.
- The investigating agencies/ police can prove the contents of the searched and seized documents either by primary or secondary evidence in a Court of Law.



## Legal Foundations that drive these actions

The power to conduct search and seizure is derived from various laws such as [6]:

- + The Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) [7]
  - + The Bharatiya Sakshya Adhiniyam, 2023 (BSA) [8]
- + The Bharatiya Nyaya Sanhita, 2023 (BNS) [9]
  - + The Income Tax Act, 1961 (ITA)
- + Unlawful Activities (Prevention) Act, 1967, and (UAPA)
  - + Prevention of Money Laundering Act, 2002 (PMLA)
- + CBI Manual of 2020
  - + The Information Technology Act, 2000 (IT Act)
- + The Telecommunications Act, 2023
  - + The Narcotic Drugs And Psychotropic Substances Act, 1985

# BEHIND-THE-SCENES: WHO'S WHO OF SEARCH & SEIZURE

The authority competent to conduct Search and Seizure differ across legislations and are as follows. The purpose of this section is to give general information on who has the authority to issue the order for the search. Perusing this will help you pursue the appropriate line of questioning with the investigating authorities.

Different laws and situations might change how searches and seizures are conducted.

## I. WHO HAS THE AUTHORITY TO ISSUE THE ORDER FOR THE SEARCH?

<b>BNSS</b>	A judge (District Magistrate, Sub-divisional Magistrate or Magistrate of the first class) can give a special permission to a police officer above the rank of a constable (not just any officer!) to search a place if they think it's hiding stolen goods or dangerous things. This officer can also get help from others if needed.
<b>Income Tax Act</b>	The Director/General/Chief Commissioner/Commissioner has the authority to issue the order for the search.
<b>UAPA</b>	The Central Government/State Government may order for the search. However, the law does not specify which wing/ Ministry of the Government (Central/State) is empowered to issue this order.
<b>PMLA</b>	<b>For Surveys:</b> Adjudicating Authority can issue the order. <b>For Seizures:</b> Director or any other officer not below the rank of Deputy Director can issue the order.
<b>IT Act</b>	The Central Government has the authority to order any officer of the Central or State Government to search. The Controller can also order a search to access data within computers.

# BEHIND-THE-SCENES: WHO'S WHO OF SEARCH & SEIZURE

The authority competent to conduct Search and Seizure differ across legislations and are as follows. The purpose of this section is to give general information on who has the authority to conduct the search. Perusing this will help you pursue the appropriate line of questioning with the investigating authorities.

Different laws and situations might change how searches and seizures are conducted.

## II. WHO HAS THE AUTHORITY TO CONDUCT A SEARCH?

BNSS	<p>Here is the basic idea on how the law on search and seizure operates:</p> <p>The Station House Officer (SHO) or the Investigating Officer (IO) may conduct search and seizure, and in absence of them, it can be conducted by any officer authorised in writing.</p> <p><b>If someone gets arrested:</b> Police can search the place where they're caught and take anything related to the crime. Only police can do this, and they can even break open doors or windows if needed.</p> <p><b>If something suspicious is hidden:</b> A judge (District Magistrate, Sub-divisional Magistrate or Magistrate of the first class) can give a special permission to a police officer above the rank of a constable (not just any officer!) to search a place if they think it's hiding stolen goods or dangerous things. This officer can also get help from others if needed.</p> <p><b>Sections: 44 &amp; 97</b></p>
UAPA	<p>The authority to investigate UAPA is different in different cities:</p> <p><b>Delhi Special Police Establishment:</b> Deputy Superintendent of Police or equivalent.</p> <p><b>Metropolitan areas of Mumbai, Kolkata, Chennai, Ahmedabad, and notified areas:</b> Assistant Commissioner of Police and higher.</p> <p><b>Other cases:</b> Officers not below the rank of Deputy Superintendent of Police or equivalent.</p>

# BEHIND-THE-SCENES: WHO'S WHO OF SEARCH & SEIZURE

The authority competent to conduct Search and Seizure differ across legislations and are as follows. The purpose of this section is to give general information on who has the authority to conduct the search. Perusing this will help you pursue the appropriate line of questioning with the investigating authorities.

Different laws and situations might change how searches and seizures are conducted.

## II. WHO HAS THE AUTHORITY TO CONDUCT A SEARCH?

<b>Income Tax Act</b>	Only Income Tax officers not below the rank of Assistant Commissioners or higher can investigate.
<b>PMLA</b>	The Director or any other officer, not below the rank of Deputy Director has the authority to investigate.
<b>IT Act</b>	Any police officer not below the rank of an Inspector. Additionally, any other officer of the Central or State Government can be authorised by the Central Government to investigate. The Controller or any other officer authorised by them can also investigate.
<b>Telecommunications Act, 2023</b>	This law empowers an authorised officer of the Central Government to search any place if such an officer has a reason to believe that any unauthorised telecommunication network or equipment has been kept or concealed. <b>[10]</b>



**section 2**

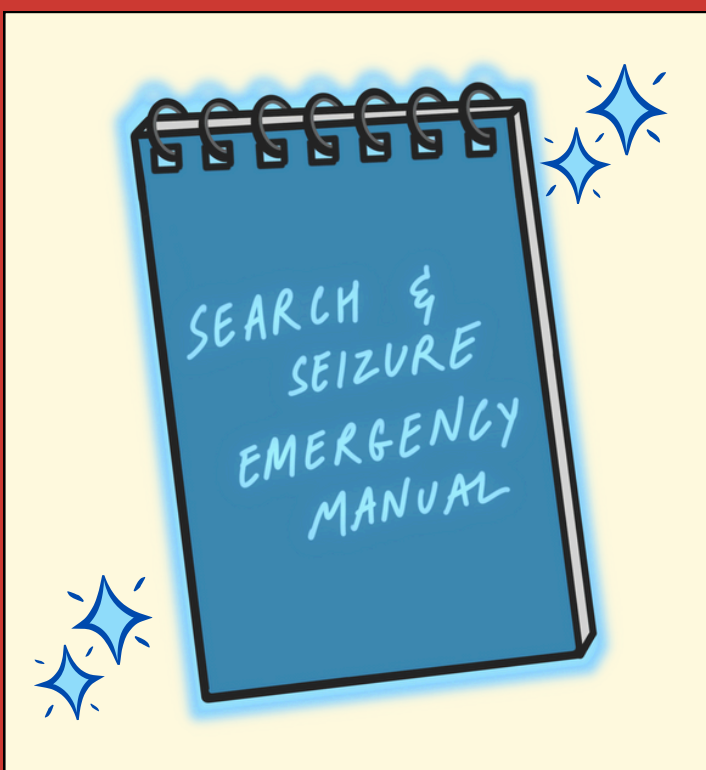
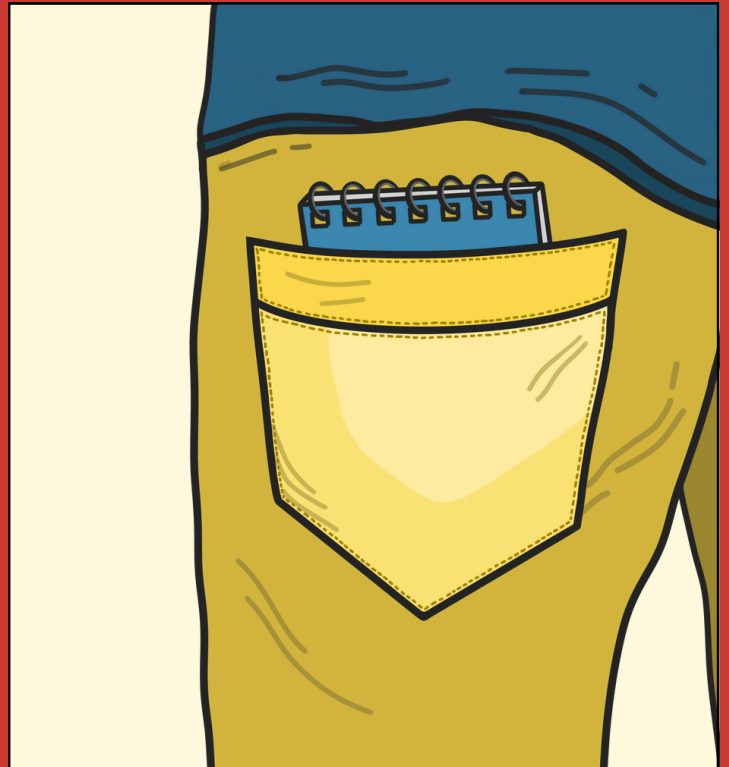
# **WHAT TO DO DURING A SEARCH?**



**The process of conducting an investigation can be complex and daunting.**

To navigate this process effectively, it is essential to understand the procedures involved and the necessary documentation.

An investigation may ultimately result in a trial, and in such cases, a thorough understanding of search procedures and related protocols can be crucial for defending oneself in court.





**During the beginning of the search, these questions can come in handy**



1	<b>Do you have a warrant?</b>
2	<b>Has it been served electronically?</b>
3	<b>If yes, then through which medium?</b>
4	<b>Which investigating agency do you represent?</b>
5	<b>What is your designation?</b>
6	<b>What are the allegations against me?</b>

In addition, please keep in mind that -If you feel that your questions are not being answered properly, contact an advocate immediately. It is advised that you **don't** answer any further questions until your legal representative is present.

### **Extracting information effectively from the authorities.**

- The police can search your electronic devices – with or without a warrant. **However, you should always ask for a copy of the recording of the procedure of search and seizure from the nearest Magistrate [11] – who has received such a recording from the police officer. [12]**
- **You can also refuse to provide electronic records of any other person in your possession unless the same person consents to it.**
- Search and Seizure is a standard procedure in any investigation, merely because your house and devices are being searched **does not mean** that you are guilty. If the investigating agencies have complete documents authorising them to conduct the search, let them do their job. Contact your lawyer as you may need him/her in the future.
- The investigating authorities may not respond to your questions at times, it is best that you note down your questions and the responses on a piece of paper, so it can be used further in a trial.
- You are under no obligation to assist the Investigating Agencies with their Search, however, you are not supposed to interfere in the process either. This means for example running away with the device or breaking the device.

During the search and seizure at the site, analysis involves the immediate examination and evaluation of collected evidence to ensure its relevance and integrity.

This includes reviewing and documenting physical items and digital devices found at the scene, performing data extraction and forensic analysis to recover and verify information while preventing tampering. Key patterns and connections are identified, and detailed notes are taken to maintain a clear chain of custody.

1	<b>Keep a List of Devices and accounts used for analysis:</b>  Maintain a list of devices and accounts used for analysis of the searched devices to facilitate cross-referencing of all data collected by the officers later.
2	<b>Do not disclose the storage locations of files on your devices:</b>  When authorities conduct a search and seizure, it is advisable not to disclose the storage locations of files on your devices to protect your privacy and the integrity of the process. Providing information about where the files are stored could inadvertently expand the scope of the search beyond what is legally permitted, and would potentially expose sensitive or irrelevant personal information.
3	<b>Keep note of all IMEI, serial numbers, and specifications of all devices taken for analysis:</b>  This helps verify the device's identity, prevents mix-ups with other devices, and maintains the integrity of the evidence by confirming that the correct item is being analysed or presented in court.

## **section 3**

# **ELECTRONIC DEVICES AND THE LAW**

The Supreme Court of India in *K.S. Puttuswamy v. Union of India* (2017) recognized privacy including informational privacy as a fundamental right [13] – In *Virender Khanna v. State of Karnataka*, the Karnataka High Court prescribed broad guidelines on the search and seizure of electronic devices. In this case, the Court ruled that divulging a password, biometrics, passcode to provide access to a smartphone or a computer system will not violate the fundamental right against self-incrimination of a person.[14]

However, the Foundation of Media Professionals had moved the Supreme Court, arguing that the law – at present – is inadequate in protecting people from the violation of their fundamental rights against self-incrimination and privacy – considering electronic devices store a great amount of personal data of a person.[15] A committee was formed to develop guidelines on the search and seizure of electronic devices by investigative agencies.[16]

Please go through the Annexure if you want to know how the process of search and seizure is conducted under various laws.



**section 4**

# **POST-SEIZURE PROTOCOL:**

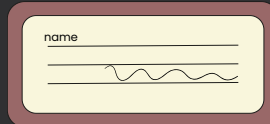
**What happens once your  
device is seized?**

# MUST-HAVE DOCUMENTATIONS FOR SEIZED DEVICES

## Certificates

[under Section 63(4)(c) of the BSA]

One can request a copy of the **Certificates to be filed by the person whose device(s) is being searched and seized and the expert who has been conducting the procedure [17][18]**, which should detail:



**Name of the person whose device has been searched and seized and signature**



**Date and time of seizure**



**Location of seizure**



**Description of seized devices (make, model, serial number/IMEI/UIN/UID/MAC)**

**0000 1111  
0000 2222**

**HASH value (along with a Hash report)**



**Certificate to be filed by expert & duly signed with all relevant details**



**Names of witnesses present during the seizure**



**Reason for seizure**



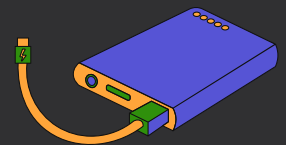
Request that the search and seizure procedure be recorded electronically or most preferably by mobile phone.



Request a copy of the recording once the Magistrate has it.



## Inventory List



Ask for a detailed **inventory list** [19] of all items seized, including any accessories like chargers or cases.

## Reasons for Seizure



Clearly inquire about the **specific reasons** why your devices were seized and the provisions of the law under which the seizure was done.



## Access to Legal Counsel

Assert your right to **consult with a lawyer** while the search is taking place.





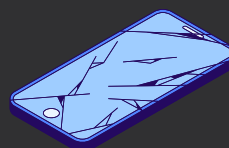
## Copies of Warrants/Orders:

If the seizure was based on a warrant [20] or order from a magistrate, request **copies of the documents** authorising the seizure. Check whether the Warrant/Order contains the correct details of the intended persons, if it is signed by the relevant Authorised Officer.



## Estimated Duration of Seizure

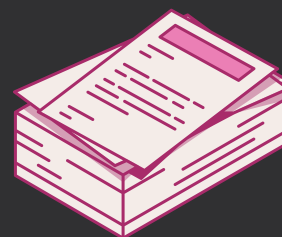
Inquire about the **estimated duration** the devices will be held and the process for their return.



## Document-ing the Condition

Before handing over your devices, ask to **document their condition** (e.g., scratches, dents) with photos or videos.

## Additional documents




Depending on the circumstances, you may request additional information such as:

- Details of the investigating officer in charge
- Information about the complaint or case related to the seizure including the case number
- Copies of any relevant policies or procedures the authorities followed


## WHAT IF YOUR DEVICE IS NOT RETURNED FOR A LONG PERIOD?

- \* The procedure on how your device will be returned will depend upon whether it was produced before a Court. Suppose your device was produced before a Court during an inquiry or trial. In that case, the Court can order its return after the inquiry or trial has been concluded, as per Sections 497 and 503 of BNSS, 2023. Section 497 has been elaborated and specifies a time frame now.
- \* However, if your seized property was not produced before a Court and if the Magistrate deems fit, they will issue a return order that your devices are ready to be collected, for which you have **six months** to claim it. [21]


In any situation, it is possible that the process to claim seized property by the police could vary depending on the particular circumstances of your case. In either of these situations, if your device is ready to be collected and you are facing issues in doing so, then remember that the process for claiming seized property by the police varies depending on the specific circumstances of your case. However, here's a general overview of all the steps you can take:



**Gather information:** Make a list of the specific items that were seized, including any identifying information like serial numbers, descriptions, specifications, etc. and any documents that prove your ownership of the property, such as purchase receipts, bills of sale, or registration certificates.



**Contact the police station:** Once you have gathered the necessary information, visit the nearest police station, either where the case has been filed or where your property was seized. Speak to the Officer-in-Charge, or Investigating Officer or any personnel in the property department. Explain your situation and request the return of your property. Be patient, polite and cooperative, and present any relevant documents you have.



**Seek legal assistance:** If the police are not cooperative or the process seems complex, consider seeking legal assistance from a lawyer.

# POST-SEIZURE CHECKLIST FOR WHEN YOUR DEVICE IS RETURNED

## 1. GENERAL INSPECTION

### Devices & Services

Obtain a list from the officers detailing all the devices they have analysed or seized, as well as the services they have examined, such as email, chat, etc so you can cross-check with your pre-seizure database.

### Startup & Functionality

Power on the device and ensure it boots up normally. Test the basic functions and features, like internet connectivity, app usage, camera, etc.

### Device Return

Ensure that after the seizure, all devices that were not seized are returned to you.

### Physical Condition

Check for any physical damage to the device, including signs of tampering with seals or screws. Take pictures/document any suspicious marks or damage to the device.

### Settings & Configurations

Check if any settings, access controls or configurations have been changed, particularly in security, privacy, or location services.

# POST-SEIZURE CHECKLIST FOR WHEN YOUR DEVICE IS RETURNED

## 1. GENERAL INSPECTION

### Installed Software/ Apps

Check if any new software or operating system has been installed on your phone and compare the list of installed apps to what you remember before the seizure. Unknown or suspicious software or applications could be signs of spyware and/or malware.

### Unusual Activity

Any indescribable or unusual activity with your device, such as excessive battery draining, data use, dysfunctional features, etc. could be signs of spyware and/or malware.

### Online Accounts

Check your online accounts such as email, online storage, social media etc. to see if any other devices are logged in that are not used by you. If you find any unfamiliar devices, take immediate action to remove them to secure your account. This can usually be done through the account's security settings.

# POST-SEIZURE CHECKLIST FOR WHEN YOUR DEVICE IS RETURNED

## 2. DATA INTEGRITY

### Data Verification

Verify that all your data is intact. Check files, photos, documents, metadata and any other data to ensure nothing is missing or corrupted.

### File Timestamps

Examine the timestamps of critical files and documents on your device as tampered timestamps could point to unauthorised access or modification.

### File Hashes

Generate and compare cryptographic hashes of important files before and after the seizure. Discrepancies might indicate file alteration or replacement.

### Forensic Tool Scans

Consider using anti-malware and forensic software to scan your device for hidden files, traces of spyware, or rootkits. These tools can be complex, so consulting a data recovery or cybersecurity specialist might be helpful.

# POST-SEIZURE CHECKLIST FOR WHEN YOUR DEVICE IS RETURNED

## 3. ADDITIONAL CONSIDERATIONS

### Backup Logs

If your device supports it, check if any backup logs or system logs show unusual or unauthorised activity during the seizure period.

### Cloud Storage

Review your cloud storage accounts associated with the device for any unauthorised access or changes.

### Document -ation

Keep a detailed record of your findings, including timestamps, screenshots, and notes on any suspicious activity. This documentation can be crucial if you need to take legal action.

### Password Management

Change all your existing passwords associated with your device and any online accounts as a copy of your passwords could have been retained by the authorities.

**section 5**

# **PREPAREDNESS:**

**Safeguarding your devices**



In today's digital age, our devices store and manage vast amounts of data.

It is crucial to safeguard devices to ensure that our data remains protected.



Being prepared for these threats is simple and crucial. Imagine the chaos if your phone got hacked and all your messages were exposed! By using strong passwords, being cautious about what you share online, and keeping software up-to-date, you build a sturdy digital padlock for your suitcase. Remember, a little vigilance goes a long way in keeping your online life safe. Given below are a few good methods to keep your data safe.

## KEEP YOUR ONLINE ACTIVITY PROTECTED | Here's how:

### Cloak Yourself



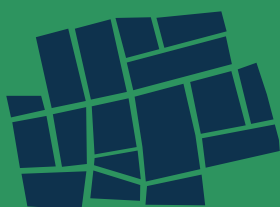
You can shield your online activity through the use of VPNs and Tor. This is akin to how a secret agent uses a disguise during a secret mission.

### VPNs



Imagine a secure tunnel for your internet traffic. It hides your real location and encrypts your data, making it like a secret code only you and the VPN can crack. Choose a trusted VPN service that doesn't log your activity.

### Tor



Picture a maze of secret pathways. Tor bounces your internet traffic through layers of encrypted relays, making it nearly impossible to track. Download the Tor Browser for extra privacy.

### Choose Wisely



Not all search engines are created equal. Some, like DuckDuckGo, prioritise privacy and don't track your searches. Even if your browser logs history, using a search engine with POST requests keeps your queries hidden.

## Go Incognito



Think of "Incognito Mode" in your browser as a secret agent's mask. It prevents your browsing history, cookies, and form data from being saved, making it hard for anyone to snoop on your online adventures.

## Stay Alert



Remember, even with these tools, absolute privacy is a myth. Be cautious about the websites you visit, always prefer secure connections (look for the lock icon!), and avoid sharing personal details online unless absolutely necessary.

## Speed vs. Privacy



VPNs and Tor can slow down your internet a bit due to encryption and rerouting. It's a trade-off: a little less speed for a lot more privacy. Choose what works best for you.

### Bonus Tip:

Always check the privacy policies and terms of service of any tool you use to understand how they handle your data. By following these simple steps, you can take control of your online privacy and keep your digital life under your own lock and key.

## WORK DEVICES VS. PERSONAL DEVICES

Imagine you have two suitcases: one for your office life and one for your personal adventures. Keeping your work laptop and phone separate is like having those separate suitcases – it helps you stay organised and protects both your professional and personal worlds.



## Consider having different devices for your personal and professional life.



**A. Data Detective:** By using separate devices, you reduce the risk of intermingling personal and professional data, enhancing security and ensuring privacy for both. By using different devices for work and personal stuff, you're basically a data detective! You stop your work files from sneaking into your personal photos and vice versa. This keeps everything secure and private, like two locked suitcases with different keys.



**B. Access Control Ninja:** Clear separation helps in controlling access to sensitive work-related information, reducing the risk of accidental exposure or data breaches. Keeping your work and personal devices separate is like having a secret code for your office suitcase. Only authorised people (like you and your boss) can access your work stuff, while your personal suitcase stays private for your eyes only. This helps prevent accidental leaks or sneaky peeks, keeping your work life safe and organised.



**C. Responsibility Champion:** Separating devices ensures clear ownership and accountability for work-related activities and data. Having separate devices makes it clear who's responsible for what. It's like labelling your suitcases – everyone knows the work suitcase belongs to you at the office, and the personal one is yours to pack with whatever you like. This makes it easier to track tasks and keep things accountable, both for you and your colleagues.

Remember, keeping your work and personal devices separate isn't just about having two gadgets – it's about protecting your privacy, staying organised, and making your life easier. So go forth, be a data detective, an access control ninja, and a responsibility champion! And don't forget to label your suitcases!

**Bonus Tip:** Even with separate devices, always be cautious about what you share online and who you give access to. No system is foolproof, so stay vigilant and enjoy your digital adventures!

# GUARD YOUR DATA LIKE A TREASURE: A Guide to Encryption Layers

Imagine your data as a treasure chest filled with precious secrets.

To keep those secrets safe, you need multiple locks, right?

That's where encryption layers come in!



## Whole Chest Lock (FDE):

- Encrypt your entire hard drive, like putting a big, strong lock on the entire treasure chest.
- Use tools like BitLocker (Windows), FileVault (macOS), or VeraCrypt (third-party).



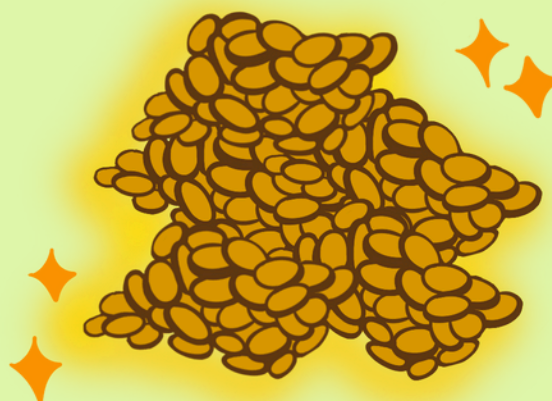
## Secret Compartment Locks (OS-Level):

- Create encrypted disk images (like secret boxes within the chest) on macOS.
- Use encrypted file systems (like hidden compartments) on some OSes.



## Individual Gem Pouches (App-Level)

- Protect specific gems (passwords, notes, messages) with apps that have built-in encryption.
- Think password managers, secure note-taking apps, and messaging apps with end-to-end encryption (e.g., Signal, WhatsApp).



### Key Reminders:

- Use strong, unique passwords or keys for each lock (encryption layer).
- Update your software regularly to keep the locks shiny and secure.
- Back up your encrypted data (treasure maps!) in case you need to find it again.



**By layering these encryption locks, you'll create a fortress for your data, making it much harder for anyone to steal your digital treasures!**







## ENSURING PRIVACY AND CYBERSECURITY: ONLINE AND OFFLINE

➡ Utilise disappearing messaging services or applications that automatically delete sent messages after they've been viewed or after a predetermined period. Apps like Signal, Telegram, and WhatsApp, etc offer disappearing message features, ensuring that communication remains temporary and doesn't persist in chats or histories after being read or after a specified time frame.

➡ Employ a password or PIN for authentication purposes rather than using fingerprint or face ID recognition, as these methods don't require conscious mental attention or explicit consent. Utilising a password or PIN ensures that access to sensitive information or devices relies solely on user-entered knowledge, enhancing control and security by necessitating deliberate action and conscious consent for authentication.

➡ Employing a password manager to store a segment of your passwords and memorising the remainder is a good strategy for enhancing security. By storing a portion of the password in a secure manager and committing the rest to memory, you create a two-part authentication that strengthens the overall security of your accounts.



- 
- For instance, utilising a password manager to securely store a segment like "12345" and memorising the complementary part, such as "fdsjrie," enables you to construct the full password as "12345fdsjrie." This method helps balance security and convenience by combining the advantages of a password manager's encryption and your ability to recall a unique segment, making it more challenging for unauthorised users to gain access to your accounts.
- 
- Implementing 2FA (Two-Factor Authentication) significantly enhances account security. Opting for TOTP (Time-Based One-Time Password) based 2FA is preferable over SMS or Email based 2FA due to its higher level of security. TOTP generates a unique code that changes at regular intervals, usually every 30 seconds, providing an additional layer of protection against unauthorised access.
- 
- Using authenticator apps like Google Authenticator, Authy, or Microsoft Authenticator, which generate TOTP codes, is a more secure option. These apps create time-sensitive codes that are tied to your accounts and don't rely on communication channels like SMS or email, reducing the risk of interception or SIM swapping attacks that can compromise SMS-based 2FA.
- 
- By leveraging TOTP-based 2FA, you add an extra layer of security that significantly decreases the likelihood of unauthorised access to your accounts, offering more robust protection against various cyber threats.
- 
- Deleting files isn't enough to truly protect your privacy! Just clicking "Delete" doesn't make them disappear forever. They're still hiding on your device, waiting to be found with special tools. To truly keep things private, you need to shred those files. Think of it like shredding paper documents – it's almost impossible to put them back together! Shredding software overwrites your files with random letters and numbers, making them scrambled and unreadable. It's like throwing away shredded paper and burying it deep underground. No one can dig it up and read your secrets! So, next time you want to delete something sensitive, skip the "Delete" button and grab some shredding software. It's the best way to keep your digital life private and secure.
- 
- Accessing websites through Tor ensures enhanced privacy and security. For instance, you can visit news sites like The Guardian or social media platforms like Twitter using Tor for added anonymity.



## Hiding Stuff: Online and Offline

### Online:

- **Crypt.ee:** Allows anonymous sign up, end-to-end encryption, and creation of hidden folders for added privacy.
- **Cryptomator:** Stores files encrypted on personal servers, making file locations untraceable after app uninstallation.

### Offline:

- **Veracrypt:** Create hidden partitions for securing data on drives or storage devices.
- **Secret Compartments:** Conceal valuables in hidden compartments within furniture or objects.
- **Cipher Systems:** Develop personal codes or ciphers to encrypt and secure written information or possessions.

These methods offer enhanced privacy and security, both digitally and in physical spaces, providing ways to safeguard sensitive information.



Store rarely used files in a secure safe-place (encrypted drive or cloud) and regularly tidy up your digital desk, keeping only what you need now. Archive old versions instead of making copies, making your digital life organised and secure.



Want to join a site without leaving your digital fingerprints? Pick ones that:

- Ask for the least info: Just a username and maybe an email, like a secret handshake.
- Let you be invisible: No name? No worries! Some sites let you sign up without saying who you are.
- Offer fake email addresses: Use a "throw-away" email to join, keeping your real one private.



## GLOSSARY:

**Audio-video electronic:** It means any communication device for video conferencing, recording identification processes, search and seizure, collecting evidence, transmitting electronic communication, and other uses as specified by the State Government rules.

**Arrest:** When a person is taken into legal custody and is detained/confined, whether or not there exists any accusation or allegation that they have committed an offence, they are said to be arrested. A person can be arrested in the absence of any charges filed or even without a warrant (*see Cognizable Offences*).

**Bailable Offences:** Offences that are not too serious or grave in nature for which an accused/arrested person has the right to seek bail are bailable offences.<sup>[22]</sup> An Investigating Officer is required to grant bail for bailable offences, usually on a condition to submit a bail bond. However, granting bail doesn't mean that the accused is free as they would still need to undergo the judicial trial.

**Charge:** A charge is a formal accusation that a person has committed an offence, made by either a Prosecutor or a Police/Investigating Office.<sup>[23]</sup> This requires a person to be informed of the grounds of the charge/s against them.

**Cognizable Offences:** Offences for which a Police Officer can arrest without a warrant or prior permission from the Magistrate are Cognizable Offences.<sup>[24]</sup> This happens whether or not an FIR (First Information Report) is filed and is usually applicable for offences that are more serious or grave in nature.

**Computer:** It means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network.

**Communication device:** This can be a cell phone, a device for personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image.

**Cookies:** Small files of information/data that track and record your activity in a web browser are Cookies. They can be used for advertising and analytics services to record user activity. Cookies can contain personal information about users, such as their username and password, customised preferences, web activity, etc. and if they are unsecured, they can be a potential security and privacy risk for users.

## GLOSSARY:

**Electronic communication:** This refers to any written, verbal, pictorial, or video information shared electronically, whether between people or devices, using phones, computers, audio-video players, cameras, or other electronic devices, or any other electronic form as specified by the Central Government.

**Encryption:** The process that stores personal or sensitive data in a cryptic/code form that can only be decrypted/decoded by a person who has access to a decryption key is Encryption. This makes processing, storing and transferring personal and sensitive information more secure and protected as it excludes any unauthorised person from accessing or understanding the data.

**Evidence:** Evidence is any statement, which can be either oral or in a documented form (written or electronic and includes digital devices as well), that may be related to an inquiry or investigation. Such documents are called documentary evidence. Evidence is separate from proof, as it is not necessarily conclusive and is subject to the Court's discretion.

**Investigating Officer (IO):** A Police Officer who has been assigned to investigate a crime.

**Moveable Property:** While the BNS only defines movable property, meaning, property of every description such as window, door, trees etc, it does not include things which are attached to earth or permanently fastened to anything that is attached to earth. Moveable property shall also include all electronics and digital devices which are not attached to earth. [25]

**Non-Bailable Offences:** Offences that are more serious or grave in nature for which an accused/arrested person does not have the right to seek bail are bailable offences. Despite that they do not possess a right, the Court can still grant them bail based on its discretion based on the risk of the accused fleeing, not cooperating with legal proceedings, etc.

**Non-Cognizable Offences:** Offences for which a Police Officer cannot arrest without a warrant or prior permission from the Magistrate are Non-Cognizable Offences. [26] This happens after an FIR (First Information Report) is filed & a warrant has been obtained and is usually applicable for offences that are less serious or grave in nature.

**Place:** Under BNSS, a place can be a house, building, tent, vehicle and vessel. [27]

**Public Place:** It is meant to include any place for public conveyance, hotels, shops or any other place that is meant for use or access by the public.[28]

## GLOSSARY:

**Seizure Memo:** If any property (valuable or invaluable) is seized from an accused person by an Investigating Officer, for the purposes of investigation, it is registered and recorded in a Seizure Memo. This contains all details of the particulars/specifications/details of the property, place of storage, details of the case that the seizure is linked with, etc.

**Warrant:** A warrant is a document signed by a judge giving the police permission to either arrest you or search your property and take certain items from that property. You have the right to see the warrant and should check to make sure it is valid.

## ANNEXURE:

### Some Notes on Search and Seizure:

1. Previously, the courts have ruled that evidence obtained through illegal and improper means could be admissible. However, such evidence must be proven to be genuine and untampered in nature. Determination of admissibility can only be made by the courts – depending on the facts and circumstances of each case. [*Umesh Kumar v. State of A.P.*, (2013) 10 SCC 169]
2. However, the High Court of Kerala had ruled that a police officer cannot seize the mobile phone of a journalist without adhering to the procedure established within the CrPC (now BNSS). If such a device is necessary to the investigation of a crime, then such police officers must follow the CrPC (now BNSS) for the proper search and seizure of the device. [29]
3. The High Court of Delhi has also ruled that a person cannot be coerced to provide the password (or any other details) in view of the protection from self-incrimination in Article 20(3) of the Constitution of India.[30]
4. Similarly, a special CBI Court of a Rouse Avenue District Court in Delhi held that the accused cannot be compelled to give such information and in this regard he is protected by Article 20(3) of the Constitution of India as well as Section 180(2) of BNSS. [31]
5. Understanding Search and Seizure procedures could not only help you avoid panic in such intense situations but also help you cooperate with the authorities better. In addition, knowing such procedures can protect individuals from mistreatment by those responsible for maintaining law and order.

### Electronic Devices and the Law

The judicial position on this matter remains unsettled. However, there are general guidelines with respect to search and seizure within the BNSS, BSA, UAPA, Income Tax Act, PMLA and IT Act. It must be noted that the processes of Search and Seizure differs across these legislations and are given on the following page.

## ANNEXURE:

<p><b>Bharatiya Nagrik Suraksha Sanhita (BNSS)</b></p> <p><b>With Warrant</b></p>	<p><b>Section 96–</b> This provision requires that a police officer seeks a special permission from the court. When the court has a reason to believe that a search should be conducted, then the court specifies the conditions under which a search warrant may be issued. The officer in charge of the search/seizure should restrict himself to a specific area for which the warrant is issued.</p> <p><b>Section 103–</b> This is a basic provision for searching and seizing property. Police need to follow these rules whenever they're searching or seizing properties.</p>
<p><b>Bharatiya Nagrik Suraksha Sanhita (BNSS)</b></p> <p><b>Without Warrant</b></p>	<p><b>Section 185–</b> Police can enter and search a place without getting special permission (warrant) if they think a crime might happen soon or if it's crucial for their investigation. Also, the provision now mandates that a police officer conducting a search is required to record the procedure. An officer, if unable to conduct the search, may require his subordinate to do so after recording the reasons in writing. The copies of record of such search shall be sent to the nearest Magistrate in no later than forty eight hours.</p> <p><b>Statements during Investigations:</b> There are provisions (in <b>Sections 180 and 181</b>) that say a person doesn't have to attest to any statement they make during an investigation. Also, people have a right not to say things that might make them look guilty, protected by the Indian constitution.<sup>[32]</sup></p> <p><b>Arrests without Warrants:</b> According to <b>Section 35</b>, police can also arrest someone without a warrant if they think that person was involved in a serious crime, if there's a complaint against them, or if there is a reason to believe that they're involved in a crime. However, an infirm person or person above the age of sixty shall not be arrested without the prior permission of DSP in case where the offence is punishable for imprisonment of less than three years.</p>
	<p><b>Section 105–</b> A newly inserted provision that now requires that the police officer shall record the search and seizure proceedings preferably through mobile phone. It also requires that a list of seized items, signed by witnesses, must be prepared and the same should be promptly sent to the District Magistrate, or Judicial Magistrate of the first class.</p> <p>Police under <b>Section 106</b> have the power to take/ seize any property they think might be stolen. Sometimes, this provision gets misused for general searches, covering everything they find. It empowers any police officer to seize any property suspected to be stolen or linked with the commission of crime. The police officer must report the seizure to the local magistrate and its custody can also be granted to the responsible person on his signing bond to produce the seized property whenever it is needed in court.</p>

## ANNEXURE:

<b>Bharatiya Sakhsya Adhiniyam (BSA)</b>	<p><b>Section 168-</b> The judge has the authority to do the following -</p> <ul style="list-style-type: none"> <li>• Ask questions in relation to facts that are relevant or irrelevant - in any manner whatsoever.</li> <li>• Ask questions to any parties and witnesses at any time.</li> <li>• Demand the production of any documents or things as proof.</li> </ul> <p>Importantly, no individual can object to the requests or demands of the judge, as provided under this provision.</p> <p>[This might be crucial in cases involving search and seizure where specific documents or items could be evidence.]</p>
<b>PMLA</b>	<p><b>Sections 16 and 17-</b> These sections set out the rules for conducting a search or seizure respectively. They require a written record of why the search or seizure is happening and mandate the preparation of a report with a list of seized items. [This draws a connection between the process and documentation required during a search and seizure operation.]</p>
<b>UAPA</b>	<p><b>Section 43A-</b> Allows officers to authorise a search to subordinate officers, and mandates that the 'grounds for believing' are attributable to either personal knowledge or written information provided by a third-party.</p> <p><b>Section 43B-</b> Details the rights of the person being searched or seized. These sections ensure that during a search or seizure, the person being searched should be communicated with the grounds of their search and the things taken have to be brought to the nearest police station. The officer in charge there needs to take the necessary actions following the rules laid out in CrPC (now BNSS).</p>
<b>Income Tax Act</b>	<p><b>Section 132-</b> This section empowers authorities to seize documents or items if someone doesn't provide them as required by law. In the context of search and seizure, this section gives legal backing to the authorities to seize specific documents or items if they are not produced voluntarily during an investigation or legal proceedings. The section also provides adequate safeguards to accused persons by requiring that a fair chance must be given to the accused to provide evidence to support their explanation regarding the seized items.</p>
<b>IT Act</b>	<p><b>Section 80-</b> prescribes that authorised officers <b>[33]</b> to search any public place and arrest without warrant - any person found therein who is reasonably suspected of committing an offence under the IT Act in the past, present or the future.</p>

## ANNEXURE:

**THE SCHEDULE**  
[See section 63(4)(c)]  
**CERTIFICATE**  
**PART A**  
(To be filled by the Party)

I, \_\_\_\_\_ (Name), Son/daughter/spouse of \_\_\_\_\_  
residing/employed at \_\_\_\_\_ do hereby solemnly affirm and  
sincerely state and submit as follows:—

I have produced electronic record/output of the digital record taken from the following  
device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐  
CD/DVD ☐ Server ☐ Cloud ☐ Other ☐  
Other: \_\_\_\_\_

Make & Model: \_\_\_\_\_ Color: \_\_\_\_\_  
Serial Number: \_\_\_\_\_  
IMEI/UIN/UID/MAC/Cloud ID \_\_\_\_\_ (as applicable)  
and any other relevant information, if any, about the device/digital record \_\_\_\_\_ (specify).

The digital device or the digital record source was under the lawful control for regularly  
creating, storing or processing information for the purposes of carrying out regular  
activities and during this period, the computer or the communication device was working  
properly and the relevant information was regularly fed into the computer during the  
ordinary course of business. If the computer/digital device at any point of time was not  
working properly or out of operation, then it has not affected the electronic/digital  
record or its accuracy. The digital device or the source of the digital record is:—

Owned ☐ Maintained ☐ Managed ☐ Operated ☐  
by me (select as applicable).

I state that the HASH value/s of the electronic/digital record/s is \_\_\_\_\_,  
obtained through the following algorithm:—

☐ SHA1:  
☐ SHA256:  
☐ MD5:  
☐ Other \_\_\_\_\_ (Legally acceptable standard)  
(Hash report to be enclosed with the certificate)

(Name and signature)

Date (DD/MM/YYYY): \_\_\_\_\_  
Time (IST): \_\_\_\_\_ hours (In 24 hours format)  
Place: \_\_\_\_\_

**Figure 1:**  
*Certificate to be filled by the party*

## ANNEXURE:

**PART B**  
(To be filled by the Expert)

I, \_\_\_\_\_ (Name), Son/daughter/spouse of \_\_\_\_\_  
residing/employed at \_\_\_\_\_ do hereby solemnly affirm and  
sincerely state and submit as follows:—

The produced electronic record/output of the digital record are obtained from the following  
device/digital record source (tick mark):—

Computer / Storage Media ☐ DVR ☐ Mobile ☐ Flash Drive ☐  
CD/DVD ☐ Server ☐ Cloud ☐ Other ☐  
Other: \_\_\_\_\_

Make & Model: \_\_\_\_\_ Color: \_\_\_\_\_  
Serial Number: \_\_\_\_\_  
IMEI/UIN/UID/MAC/Cloud ID \_\_\_\_\_ (as applicable)  
and any other relevant information, if any, about the device/digital record \_\_\_\_\_ (specify).

I state that the HASH value/s of the electronic/digital record/s is \_\_\_\_\_,  
obtained through the following algorithm:—

☐ SHA1:  
☐ SHA256:  
☐ MD5:  
☐ Other \_\_\_\_\_ (Legally acceptable standard)

(Hash report to be enclosed with the certificate)

(Name, designation and signature)

Date (DD/MM/YYYY): \_\_\_\_\_  
Time (IST): \_\_\_\_\_ hours (In 24 hours format)  
Place: \_\_\_\_\_

\_\_\_\_\_

DIWAKAR SINGH,  
*Joint Secretary & Legislative Counsel to the Govt. of India.*

**Figure 2:**  
*Certificate to be filled by the expert*



## ANNEXURE:

Schedule XLVII--Form No. 121  
P. M. Form 31

**PROPERTY SEIZURE MEMO.**  
(P. M. Rule 165)

\$ Strike out which is not applicable  
(Search/Production/Recovery u/s.....)

1. \*District..... \*P.S.....  
\*Year..... \*FIR No...../SD. No..... Date.....
2. Acts and Sections.....
3. \*Nature property seized/received Stolen/Unclaimed/Unlawful Possession/  
Others.....
4. Property seized/received (a) Date..... (b) Time.....  
(c) Address of place of search/seizure/recovery.....  
.....  
(d) Description of the place of search/seizure/recovery.....  
.....
5. Person from whom seized/recovered:  
Name.....  
Father's/Mother's/Husband's Name.....  
Age..... Occupation.....  
Address.....
6. Witness :  
(i) Name.....  
Father's/Mother's/Husband's Name.....  
Age..... Occupation.....  
Address.....  
(ii) Name.....  
Father's/Mother's/Husband's Name.....  
Age..... Occupation.....  
Address.....
7. Action taken/recommended for disposal of perishable property.....  
.....
8. Action taken/recommended for keeping of valuable property.....  
.....
9. Identification required : Yes/No.....
10. Details of properties Seized/recovered : Use the appropriate prescribed form(s) and  
attach.....

**Figure 3:**  
*Property Seizure Memo*



## ANNEXURE:

2

11. Circumstances of Seizure \_\_\_\_\_

12. The above-mentioned properties were seized in accordance with the provisions of law in the presence of the above-said witnesses/\*\* and a copy of the seizure Memo. was given to the person/the occupant of the place from whom seized.

13. The following properties were packed and/or sealed and the signature of the said witnesses obtained thereon on the body of the property.

Sl. No.	Property	Name of the witnesses, whose signatures have been appended

Specimen of the seal is given below

Witness : \_\_\_\_\_

Signature \_\_\_\_\_ Signature of the Investigating Officer \_\_\_\_\_

Name \_\_\_\_\_

Rank \_\_\_\_\_

Witness : \_\_\_\_\_

Signature \_\_\_\_\_ Personal Number if any \_\_\_\_\_

Place \_\_\_\_\_ Date \_\_\_\_\_

\*\*In case of property is seized from such a place that no receipt is required to be given to anybody, this portion of the sentence should be struck off.

OGP (Forms) DTP-162-10,00,000-29-08-2005

**Figure 3.1:**  
Property Seizure Memo

## **SEIZURE LIST**

Case Reference :

1. Date and Hours of Seizure :
2. Place of Seizure / Person from whom seized :
3. Name and Address of Witnesses :  
(i) (ii)
4. Description of articles seized :  
(Appropriate PF and / or space on reverse may be used)
5. Circumstances of Seizure :
6. Signature of Witnesses & Police Officer

**Figure 4:**  
*Seizure List*

## ANNEXURE:

FORM No. 3  
WARRANT OF ARREST

(See section 72)

To ..... (name and designation of the person or persons who is or are to execute the warrant).

WHEREAS (name of accused) of (address) stands charged with the offence of ..... (state the offence), you are hereby directed to arrest the said ..... and to produce him before me. Herein fail not.

Dated, this..... day of....., 20 .....

(Seal of the Court) (Signature)

(See section 73)

This warrant may be endorsed as follows:—

If the said..... shall give bail himself in the sum of rupees..... with one surety in the sum of rupees..... (or two sureties each in the sum of rupees.....) to attend before me on the..... day of..... and to continue so to attend until otherwise directed by me, he may be released.

Dated, this..... day of....., 20 .....

(Seal of the Court) (Signature)

\_\_\_\_\_

**Figure 5:**  
*Warrant of Arrest Format (given in the Second  
Schedule of the BNSS at page 192 of Act  
published in official gazette notification)*

## REFERENCES:

- [1]** See glossary for the meaning of the word
- [2]** For explanation of search within the BNSS, see Section 49;97.
- [3]** Section 44 of the BNSS.
- [4]** Section 185(1) of the BNSS.
- [5]** For explanation of seizure within BNSS, see Sec 106, 117.
- [6]** This is not an exhaustive list of the laws. There are other laws as well which provide for search and seizure.
- [7]** Code of Criminal Procedure, 1973 (CrPC).
- [8]** Indian Evidence Act, 1872.
- [9]** Indian Penal Code, 1860
- [10]** See Section 42 and 43 of The Telecommunications Act, 2023
- [11]** Please note that such a recording can be provided to only Judicial Magistrate of the First Class, District Magistrate and Sub-divisional Magistrate.
- [12]** Sections 94, 185 of BNSS, 2023.
- [13]** K.S. Puttuswamy v Union of India (2017) 10 SCC 1.
- [14]** Virender Khanna v. State of Karnataka, Writ Petition No. 11759 of 2020 (GM-RES).
- [15]** Foundation of Media Professionals v. Union of India, Writ Petition (Crim) No, 395 of 2022, Supreme Court of India, pg 1.
- [16]** Awstika Das, Committee Constituted To Frame Guidelines For Seizure Of Digital Devices : Centre Tells Supreme Court, (December 6th, 2023 12:05 PM)  
<https://www.livelaw.in/top-stories/supreme-court-seizure-journalists-digital-devices-centre-243831>
- [17]** Certificate has been provided under Section 63(4)(c) of BSA, 2023.

## REFERENCES:

- [18]** A sample of the seizure memo is provided in the Annexure as Figure 3 & Figure 3.1. The source of this sample is <https://odishapolice.gov.in/sites/default/files/PDF/PROPERTY-SEIZURE-MEMO.pdf>
- [19]** A sample of such an inventory list (can be identified as the seizure list in Figure 4) is provided in the Annexure below.
- [20]** A sample of the warrant of the arrest is provided in the Annexure as Figure 5.
- [21]** BNSS Section 503(2).
- [22]** See BNSS Section 2(c).
- [23]** See BNSS Section 2(f), charge is defined under Section 2(b); See also (for better understanding of the contents of a charge) Section. 234.
- [24]** See BNSS, Section 2(g). See also First Schedule, Point (2) of Explanatory Notes, page 158 of Act published in Gazette notification.
- [25]** BNS Section 2(21).
- [26]** See BNSS Section 2(o). See also First Schedule, Point (2) of Explanatory Notes, page 158 of Act published in Gazette notification.
- [27]** BNSS, Section 2(s).
- [28]** IT Act, Explanation to section 80(1).
- [29]** G. Vishakan v. State of Kerala & Ors., WP(C) No. 22328 of 2023 (10.07.2023 - KERHC) : MANU/KE/1872/2023.
- [30]** Sanket Bhadresh Modi vs CBI, BA No. 3754/23.
- [31]** CBI vs. Mahesh Kumar Sharma, CBI 31/2021
- [32]** This right is enshrined within Part III of the Constitution of India, under art. 20(3).
- [33]** Authorised officers here means either a police officer (not below Inspector) or any other officer of the Central or State Government authorised by the Central Government.



Email: [mail@sflc.in](mailto:mail@sflc.in)

Website: <https://www.sflc.in>

*sflc.in*

