Document the device and all collection procedures and information.

<table>
<thead>
<tr>
<th>Photograph OR Video OR Sketch</th>
<th>Notes</th>
<th>Chain of custody</th>
</tr>
</thead>
</table>

Determine if the device is on or off.

- Look for lights
- Listen for sounds
- Feel for vibrations or heat

Note: Many mobile devices save power by turning off screens after a specified amount of time. Despite the screen status, the device is likely still active. Ask if the device is currently powered on. Where legal, pressing the power button quickly will activate the screen.

If the device is off, **do NOT** turn it on.

- Collect and package (see Step 5)
- Ask for password/pass pattern
- Transport (see Step 6)

If the device is on, proceed with **CAUTION**.

**WARNING**

The two most significant challenges for officers seizing mobile devices are: (1) isolating the device from cellular and WI-FI networks; and (2) obtaining security passwords or pass patterns for the device so the evidence can be examined forensically. Always ask if there is any security feature enabled on the phone. These can include passwords (simple or complex), security/wiping apps, pass patterns, or biometrics (facial scan). Document (see the attached consent form for guidance) and confirm the password or pass pattern. Turning the device off could result in the loss of evidence. The best option is to keep the device powered, unlocked (if locked, collect any available passwords, PIN codes, or security unlock information), and in airplane mode until it is in the hands of an experience technician.

Collection and Package

**WARNING**

You may need to collect other forensic evidence including fingerprints, biological samples, DNA, etc. from smart phones and mobile devices. Work with crime scene technicians or trained forensic personnel to preserve such evidence without disturbing the integrity of the data on the device. Be sure to advise forensic examiners in advance of submission of the possible existence of hazardous material on the device.

- Secure data and power cables
- Consider collecting computers that may contain device backups
- Package the device so it will not be physically damaged or deformed
- Package the device in evidence bags or boxes

Transport.

- Deliver evidence to a secure law enforcement facility or digital evidence laboratory as soon as possible
- Protect from temperature extremes and moisture

*Information provided by Massachusetts Digital Evidence Consortium*