



TR Stockwood, IT Consultant

When law enforcement investigates spying or unauthorized surveillance of a child, they treat it as a high-priority digital and physical safety threat. Because modern "spying" often involves both software (stalkerware) and physical behavior, the investigation is typically multi-layered.

Here is how the process generally unfolds:

1. Initial Triage and Risk Assessment

When you report the concern, the first step is determining if there is an **immediate physical threat**.

- **Emergency Response:** If the spying suggests an imminent abduction or physical harm, local police will coordinate with specialized units like the **FBI's CARD (Child Abduction Rapid Deployment)** teams or local **ICE (Internet Crimes Against Children)** task forces.
- **Safety Planning:** Officers may advise you to stop using certain devices immediately or move to a secure location while the investigation begins.

2. Digital Forensic Analysis

Since most spying occurs through devices, investigators look for "digital fingerprints."

- **Device Examination:** Specialists scan phones, tablets, and computers for **stalkerware** or **RATs (Remote Access Trojans)**. These programs can secretly record audio, activate cameras, and track GPS.
- **Network Audits:** They may analyze your home Wi-Fi logs to see if unauthorized devices are connected or if data is being "exfiltrated" (sent) to an outside IP address.
- **Account Logs:** Investigators subpoena records from companies (Google, Apple, Snap, etc.) to see if someone is logged into your child's accounts from an unrecognized device or location.

3. Identifying the Source

Once the method is found, the goal shifts to "who."

- **IP Tracking:** Law enforcement uses subpoenas to track the IP addresses associated with the spying software back to a physical address or a specific internet service provider (ISP).

- **Financial Trails:** If the spying was done via a paid "parental control" app used maliciously, they can often trace the credit card or account used to purchase the subscription.
- **Metadata:** Photos or files sent by the spy often contain hidden metadata (EXIF data) that reveals the exact GPS coordinates and device model of the sender.

4. Physical Investigation

If the spy is local, police move into traditional investigative techniques:

- **Surveillance:** They may monitor your home or the child's school to see if anyone is physically following or watching.
- **Interviews:** Investigators conduct "forensic interviews" with the child using specialized techniques designed to be non-traumatizing while gathering accurate evidence.
- **Search Warrants:** If a suspect is identified, police will execute search warrants to seize their devices for a "match" with the data found on your child's devices.

Important Evidence Steps for You

If you suspect spying, law enforcement recommends several "do's and don'ts" to preserve the case:

- **Do Not Factory Reset:** This erases the very evidence (logs and software) needed to catch the person.
 - **Document Everything:** Keep a log of strange occurrences (e.g., "Someone mentioned a private conversation we had in the kitchen," "The phone gets hot when not in use").
 - **Take Screenshots:** If you see strange messages or unauthorized login alerts, take a photo of the screen with a *different* camera.
-