**Types of IPDRs Obtainable from Telecom Service Providers:**

**1. Standard IPDR (Session-level Data)**

Captures basic session-level details for all internet activity over a period.

**Columns:**

|  |  |
| --- | --- |
| **Field Name** | **Description** |
| Subscriber IP | User's IP address assigned by the TSP |
| Start Time | Session start timestamp |
| End Time | Session end timestamp |
| Source Port | Port number at subscriber end |
| Destination IP | IP address accessed |
| Destination Port | Port number on remote server |
| Protocol | e.g., TCP, UDP |
| Bytes Sent | Data uploaded |
| Bytes Received | Data downloaded |
| Application Type | WhatsApp, Instagram, etc. (based on DPI or port classification) |
| ILD Flag | International Long Distance (Yes/No) |
| IMEI / Device ID | Device identifier |
| MSISDN / Mobile No. | Subscriber’s phone number |
| Cell ID / Tower ID | Tower used for internet session |
| Location (Lat, Long) | Geo-location derived from cell tower |
| Session ID | Unique session identifier |

**2. Application-specific IPDRs (OTT, Social Media, etc.)**

Detailed records filtered by app usage.

**Common Applications:**

* WhatsApp
* Instagram
* Telegram
* Facebook
* YouTube
* ChatGPT / OpenAI
* Zoom/Skype

**Additional Fields:**

|  |  |
| --- | --- |
| **Field Name** | **Description** |
| App Signature | Identifier of app (based on DPI or domain/IP mapping) |
| App Version (if detectable) | In some cases, the OS/app version may be flagged |
| FQDN / URL Accessed | Domain name (e.g., api.whatsapp.com) |
| TLS Handshake Info | If available, handshake metadata (without decrypting content) |

**3. VoIP-Specific IPDR**

Covers VoIP activity (WhatsApp call, Skype, Signal, SIP-based calls).

**Columns:**

|  |  |
| --- | --- |
| **Field Name** | **Description** |
| Source/Destination IP | IPs involved in call |
| Call Start/End Time | Duration of call |
| Call Type | Audio, Video |
| Codec Used | If detectable |
| Jitter/Latency | Quality metrics (if available) |
| Packet Loss Rate | Voice quality metric |
| Protocol | SIP, RTP, SRTP |

**4. CDR-Integrated IPDR**

Some TSPs provide combined Call Detail Records (CDRs) and IPDR views for complete profiling.

**Columns Include:**

* All CDR fields: Called/Calling party, Tower, Duration
* Mapped IP sessions during or immediately after voice/SMS session
* Social media app data around the time of call

**5. Geo-location Enriched IPDR**

Used to derive location trail of a suspect.

**Columns:** | Timestamp | App | Tower ID | Location (Lat, Long) | Direction of Movement | Duration |

**Legal Request Format**

Typically, LEAs must provide:

* MSISDN / IP / IMEI
* Time period
* Jurisdictional approval or court order (under Section 69 of IT Act, or relevant Rule 419A of Telegraph Rules)

**Summary Table of Types**

|  |  |  |
| --- | --- | --- |
| **IPDR Type** | **Key Focus** | **Used For** |
| Standard Session IPDR | Internet sessions | Broad surveillance, profiling |
| App-specific IPDR | OTT usage | Behavioral analysis |
| VoIP IPDR | Voice/video over IP | VoIP crime (sextortion, VoIP fraud) |
| CDR-integrated IPDR | Voice + data correlation | Contextual investigations |
| Geo-tagged IPDR | Movement and location trails | Suspect tracking, cross-border movement |

**Notes:**

* Actual **content of communication is** **not provided** without lawful interception authorization.
* **IPDRs are metadata**, admissible under proper legal process.
* Formats may vary slightly among **Airtel, Jio, Vi, BSNL**, etc.