



Surveillance Use Policy

CellHawk

San Diego Police Department

PURPOSE

CellHawk is specialized mapping software designed to ingest files containing location-based cell phone data for easy visualization and subsequent analysis.

USE

CellHawk is used in investigations to visualize location-based data for analysis. Once a file has been uploaded into the system, individual data points are symbolized on a map. Detectives and Crime Analysts utilize this symbolic visualization to determine either the general or specific whereabouts of a cellular device and/or subject, which informs an investigation. Locational data may also be provided on a 15-minute regular interval from a service provider using email updates.

This data is used in active investigations typically associated with exigent circumstances. Exigent circumstances are emergencies requiring law enforcement action prior to obtaining a search warrant (i.e., kidnapping, pursuit of a violent suspect, etc.). In this instance, Cellhawk would be utilized to map live ping transactions of an individual's phone. Note the cell phone carrier provides the ping locations, and Cellhawk is used solely for mapping the provided locations. After an exigent situation has been resolved, an after-action search warrant is required.

Department procedures associated with CellHawk are:

- 1.45 - Use of City / Department Computer Systems
- 4.13 – Non-Official or Personal Custody of Records/Files/Recordings Policy

DATA COLLECTION

Data retained in CellHawk is limited to the files that are uploaded into the system by either SDPD Detectives or Crime Analysts. This data is obtained via search warrants written and submitted by the case detective to the appropriate carrier. Uploaded files are organized by case and housed in a folder specifically created for that case. Files can be viewed or deleted as deemed necessary by the Detective and / or Crime Analyst assigned to the case.

DATA ACCESS

Individuals using CellHawk for investigative purposes are either SDPD sworn Detectives or SDPD civilian Crime Analysts, assigned to a case.

DATA PROTECTION

Computers in SDPD secure law enforcement facilities require a user's approved CellHawk login credentials to access the system. Per Leads Online, data is protected within their secure environment:

"Leads requires passwords in order to access Leads' System and Data."



Surveillance Use Policy

CellHawk
San Diego Police Department

Leads provides for 256-Bit Transport Layer Security (TLS) encryption in order to protect the Data against the interception and unauthorized use of information. The actual encryption strength is determined by the level of encryption supported and selected by the user's browser.

Data is secured behind firewalls isolating it from web servers in order to prevent unauthorized electronic access.

Leads uses qualified systems and services in order to identify possible security vulnerabilities.”

DATA RETENTION

Data retained in CellHawk will remain for the duration of the investigation, or however long the Detective assigned to the case deems it necessary to retain. Deletion of files can be performed by either a Detective or Crime Analyst assigned to a case. Evidence or investigative records shall be maintained in Cellhawk for the duration of an investigation in accordance with DP 4.13 – Retention/Custody of Officer Notes, Documents, and Other Evidence.

PUBLIC ACCESS

The general public has no access to the CellHawk system or information contained in the database.

THIRD PARTY DATA SHARING

Data retained in CellHawk can be accessed by analysts working for Hawk Analytics. Typically, the scenario in which this would happen involves the user (Detective or Crime Analyst) reaching out to Hawk Analytics for assistance on either uploading a file into the system or interpreting the results once an upload is complete.

Every Cellhawk (Leads Online) employee is required to meet Criminal Justice Information Services (CJIS) certification standards in order to work with the application. No vendor analysts have access to the underlying data available in a specific agency's profile with the exemption of exigent support. Two of the Cellhawk analysts are designated as certified exigent support staff and have the ability to view data on an agency's profile if the agency grants permission. However, this permission would only be granted on a specific basis for work on a specific case and not be granted for the entire agency's available data.

TRAINING

Individuals are trained to use CellHawk in one of three ways (often in combination). Hawk Analytics provides in-person training classes, nationwide, based on user ability (beginning, advanced, etc.). Additionally, Hawk Analytics offers online webinars (“Hawk University”) that cover basic to advanced usage, as well as targeted content related to the analysis of location-based data. Lastly, Detectives and Crime Analysts are trained in-house by senior members among their ranks who have extensive experience using this system.



Surveillance Use Policy

CellHawk

San Diego Police Department

AUDITING AND OVERSIGHT

The administrator for CellHawk can request Hawk Analytics to run an audit of CellHawk users to determine the frequency of usage, per user. Users who no longer participate in investigations are removed from access and their account is reassigned to a current investigator.

Cellhawk will be audited on a regular basis as dictated by the Department's forthcoming audit schedule, overseen by the Special Projects and Legislative Affairs unit.

MAINTENANCE

CellHawk is maintained and updated as necessary by Hawk Analytics.