INTRADEPARTMENTAL CORRESPONDENCE

June 4, 2025
1.10

TO: The Honorable Board of Police Commissioners

FROM: Chief of Police

SUBJECT: 2024 ANNUAL COMPREHENSIVE TECHNOLOGY REPORT, SPECIAL ORDER NO. 11, AUGUST 17, 2022

RECOMMENDED ACTION

It is recommended that the Board of Police Commissioners REVIEW and APPROVE the Department's 2024 Annual Comprehensive Technology Report (CTR).

DISCUSSION

In 2022, *Department Manual Section 1/140.15, Acquisition and Annual Reporting of Certain Information Systems and Technologies,* was established to monitor and evaluate the use of new systems and emerging technologies by the Department. For this policy, "technology" means systems, hardware, or software, including data aggregators, that are owned, licensed, used, or shared by or with the Department and can access non-public places or information, or that aggregates publicly available information that can reveal considerable personal information about individuals.

These technologies play a crucial role in equipping officers with investigative and enforcement tools to deter crime and provide evidence for investigation, improving the Department's performance in solving crimes and bringing those responsible to the criminal justice system. In addition, the established policy provides transparency and considers the potential impact on civil liberties and constitutional rights while implementing appropriate safeguards and oversight mechanisms to protect those rights.

The CTR records the applicable technologies that were implemented or were currently in use when the policy was established. It's important to note that the following technologies have specific Department policies governing their use, and they require comprehensive periodic audits that are reported to the Board of Police Commissioners.

- Automated License Plate Reader systems
- Photo Comparison Technology
- Small Unmanned Aerial Systems

Should you have any additional questions, please contact Captain Anthony Espinoza, Innovation Management Division, at (213) 486-0270.

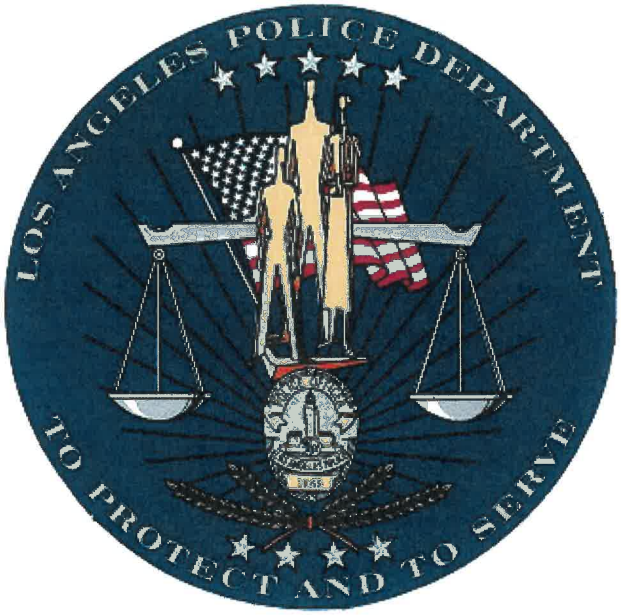
Respectfully,

JIM McDONNELL
Chief of Police

Attachment

LOS ANGELES POLICE DEPARTMENT

COMPREHENSIVE TECHNOLOGY REPORT



Completed by

INFORMATION TECHNOLOGY BUREAU

JIM McDONNELL
Chief of Police

May 16, 2025

TABLE OF CONTENTS

Comprehensive Technology Report
ITB

COMPREHENSIVE TECHNOLOGY REPORT

Completed by
Innovation Management Division
2025

OVERVIEW

Technological developments in the law enforcement industry allow for critical real-time information to assist in criminal investigations. New and emerging technologies increasingly play a crucial role in the daily work of sworn and civilian employees, equipping them with enforcement and investigative tools. These tools improve officer effectiveness and keep our communities safer. At the same time, such technologies can cause public concern about the amount of data being collected, maintained, and used by the Los Angeles Police Department (LAPD).

BACKGROUND

It is the Department's mandate to govern the adoption, deployment, and use of technology to improve community safety while protecting the civil liberties of individuals and their reasonable expectation of privacy. Affording protections for data collected, stored, and used is essential to ensure the effective and sustainable implementation of new technologies while maintaining public trust. The purpose of this report is to comply with the requirements outlined in Special Order No. 11, August 2022, for reporting new technologies.

REPORTABLE TECHNOLOGIES

A. Automated License Plate Readers

Automated License Plate Readers (ALPR) is a technology that uses optical character recognition to read vehicle license plates and record vehicle location, date, and time data. This technology can scan license plates faster than human operators. Using computer algorithms, each scanned license plate is checked against crime databases. The ALPR technology alerts law enforcement officers if a "hit" occurs (e.g., a stolen vehicle, an AMBER alert, or an arrest warrant).[1]

The Department is deploying two types of ALPR systems: mobile and fixed cameras. Mobile cameras are installed in police vehicles, trailers and smartphones. Fixed cameras are attached to stationary locations. The ALPR system consists of the following three components:

- A camera that captures license plates within its field of view as well as the dates, times, and locations associated with the photos;
- Software that reads and converts images of license plates into data; and
- A searchable database that stores the data.

[1] A "hit" refers to a match between a license plate and a system alert tied to the specific license plate.

On January 22, 2022, the Department contracted with Vigilant Solutions (Vigilant), a subsidiary of Motorola Solutions, for a new mobile ALPR system. Additionally, in 2023, the Department upgraded the Axon Fleet 3 Digital In-Car Video System (DICVS) with an ALPR feature and began using Flock Safety's (Flock) user interface to view Flock data.

- Vigilant
  On January 22, 2022, the Department signed a contract with Vigilant to replace outdated cameras with new mobile ALPR systems. The contract is for five years and involves the installation of 28 mobile ALPR cameras per year, totaling 140 mobile ALPR cameras across all geographical areas and traffic divisions, at the completion of the contract in 2027. As of the end of 2024, 84 Vigilant mobile ALPR cameras have been installed on vehicles. Additionally, 160 Vigilant fixed ALPR cameras were installed across the city.

- Axon Enterprise, Fleet 3 DICVS and ALPR
  Axon Fleet 3 DICVS provides many features, and ALPR is one of them. In November 2023, the Department activated the Fleet 3 ALPR feature. Currently, 1,500 Axon Fleet 3 mobile units have been installed.

- Flock Safety ALPR Data
  Flock offers ALPR services to its subscribers, including both residential and commercial communities such as individuals, homeowners' associations (HOA), retail and wholesale businesses, shopping malls, business improvement districts (BIDs), and others. Flock owns and maintains the ALPR cameras, which are leased to the subscribers. All ALPR data collected is solely owned by the subscribers.

  On July 11, 2023, the Department and Flock signed a Memorandum of Understanding (MOU). Flock agreed to provide its ALPR data to the Department for investigative purposes, consistent with the Department's policies and the law.

This section was intentionally left blank

Findings:

1. **The Technology Met the Expectations of the Presentation to the Board of Police Commissioners and the Department when the Technology was Obtained**

   This technology assists field officers in identifying and locating specific vehicles wanted in connection with felony crimes, stolen vehicles, and other open criminal investigations. It also helps officers locate critical missing or other endangered persons. Personnel use ALPR historical data to investigate vehicles related to open cases.

   In 2024, 301,655 hits were recorded for real-time license plate scanning and data query combined (see Findings Nos. 2 and 3). Most hits were classified as felony crimes and stolen vehicle-related matches. The ALPR system has been an invaluable tool in crime prevention and investigation because of its capability to provide real-time alerts and identify criminal suspects.

2. **Frequency of Use**

   During 2024, a total of 159,326 ALPR data inquiries (queries) were conducted by Department investigators. The number of inquiries performed indicates the value of the ALPR application as a tool essential in conducting thorough follow-up investigations involving missing, at-risk, or wanted persons utilizing a vehicle.

3. **Efficacy of the Technology**

   In 2024, ALPR cameras reported 1,132,441,520 license plate detections (reads). Real-time scanning and data queries resulted in 301,655 hits. These hits only occurred with the efficiencies made possible through automation.

4. **Personnel Compliance of All End-users**

   Special Order No. 31, December 10, 2020, established Department Manual Section 3/568.53, *Automated License Plate Recognition Usage and Privacy Policy,* to ensure that all activities pertaining to the capture, use, retention, and dissemination of information obtained through the ALPR system comply with all applicable Federal, State, and local laws.[2]

   The ALPR policy restricts the use of the ALPR system. The ALPR data shall only be retained, accessed, and used for the following official Department purposes:

   - Criminal investigations or proceedings;
   - Non-criminal investigations (e.g., missing and found persons);
   - Administrative investigations or proceedings;

[2] See Special Order No. 7, *Automated License Plate Recognition Usage and Privacy Policy - Revised*, dated February 7, 2023.

- Civil litigation or proceedings;
- Situational awareness operations;[3] and
- Responses to cognizable threats to public safety.

Per Department Policy:

> All ALPR data recorded and/or retained by the Department shall not be sold, shared, transferred, or otherwise disclosed for commercial purposes or to persons or entities not authorized to record, retain, access, or use ALPR data. The ALPR data shall only be shared with local law enforcement agencies with an interagency agreement with the Department. All current and future contracts shall be reviewed and contain a clause prohibiting the sharing of Department ALPR data outside of the agency with which the Department has an agreement.
>
> Interagency agreements or Memorandum of Agreement (MOA) shall be approved and signed by the Chief of Police. The Department has MOAs with Huntington Park PD, La Mesa PD, Livermore PD, San Luis Obispo Sheriff's Dept, West Covina PD, and the Los Angeles Port Police.

5. The Cost of the Technology and Cost-Benefit Analysis

- Vigilant Solutions, Inc.
  The current five-year Vigilant ALPR contract was signed in 2022 with an annual cost of $407,000. This contract includes 140 mobile ALPR cameras, data migration from a replaced PIPS to Vigilant, access to the Vigilant system training application, Law Enforcement Archival Reporting Network (LEARN), and 10,000 user licenses. In 2022, the Department contracted for 60 fixed pole ALPR cameras and four ALPR camera trailers for $800,000 for five years. Additionally, 160 fixed ALPR cameras have been installed.

- Axon Enterprise, Fleet 3 DICVS ALPR
  Fleet 3 ALPR is an add-on feature within the current Axon contract. Currently, the ALPR feature is in a trial period and at no cost. Information Technology Bureau (ITB) and Axon Enterprise are negotiating the Fleet 3 ALPR cost and service contract terms before the trial period ends.

- Flock Safety ALPR Data Only
  The Department has no contract with Flock in 2024 and owns no Flock ALPR cameras. Flock and the Department entered into an MOU for Flock to provide ALPR data to the Department for lawful and legitimate investigations, and the data is available at no cost to the Department. The Department will be considering deploying FLOCK ALPR cameras in 2025.

---

[3] An example of a situational awareness operation is monitoring an event or environment, its elements, and how it changes with respect to time and other factors.

The technology assists field officers in identifying and capturing felony suspects, recovering stolen vehicles, conducting criminal investigations, and locating missing or endangered individuals. It provides officers with tools to perform their duties more efficiently, ultimately making our communities safer.

6. Identified Concerns and Proposed Mitigations

There were no concerns identified.

7. Efficacy of the Existing Policy and Any Proposed Changes

A review of the Department's ALPR Usage and Privacy Policy showed that it was consistent with the United States Constitution, the Fourth Amendment, and other applicable statutory authorities.

8. Efficacy of the Training on the Existing Policy and Any Proposed Changes

Two types of users are authorized to use the ALPR system: administrators and data users.

- System Administrators:
  Administrators are assigned to ITB and have the highest access rights to the ALPR system. They are responsible for verifying the system's proper operation and ensuring the maintenance of the ALPR server. The administrators are also responsible for assisting in any reports of inoperability or malfunction of ALPR-equipped vehicles.

- Training:
  All administrators shall receive Department-approved training to fulfill their job responsibilities before accessing the ALPR system. Any ALPR data user or system administrator who has not used their ALPR system account for one year shall complete a reorientation training course before accessing the ALPR system.

- ALPR Data Users:
  Data Users are any active Department employees who have received written authorization from their supervisor and have been granted permission from ITB to query the ALPR system.

- Training:
  Employees shall receive online Learning Management System (LMS) training to query the ALPR system. Once employees complete the required LMS training, the system administrator grants access to the ALPR query capability.

Note: Employees equipped with the ALPR cameras in their Department vehicles may receive an ALPR hit alert and review the alert to locate the wanted vehicle. Employees receiving the hit alert cannot query, add, remove, or change any information in the ALPR system.

Other Related Matters

Data Retention/Data Security

All license plate data collected is uploaded to a secure and fully Criminal Justice Information Systems (CJIS) compliant cloud-based storage provided by the authorized vendors. The CJIS-compliant cloud-based storage is only accessible to authorized Department personnel.

Privacy, Civil Rights, and Civil Liberties (P/CRCL)

- Potential Impact on Privacy and Civil Rights

  The Department's ALPR cameras only collect and record information available to public view. The system obtains the license plate number, date, time, and location. It does not collect vehicle owner information, registration records, or personal information. With the existing data storage security and access requirements, there is minimal impact on P/CRCL. All ALPR data inquiries are logged and limited to stated purposes and are subject to periodic inspections and audits for appropriateness.

- Measures Currently in Place to Maintain Data Security

  The data is stored in a CJIS security-compliant cloud storage. Access to data is limited to authorized Department personnel who have completed the required ALPR Data Users training. In addition, the system shall only be accessed and used for official Department purposes.

- Plan to Safeguard Privacy and Civil Rights

  The Department delineates authorized ALPR system use as listed on Page 3 – *Personnel Compliance of All End-users*. The Department requires only that the license plate be visible in public view and that no information that can substantially reveal personal information is collected or maintained. Furthermore, routine inspections are conducted by ITB to ensure the ALPR system is used in accordance with the law and policy.

- Public Access to the Data

  The public does not have access to ALPR data. The public may submit a request for information to Risk Management & Legal Affairs Division (RMLAD), Discovery Section, in accordance with the California Public Records Act (CPRA) and the Freedom of Information Act (FOIA) as the law allows.

Inspections/Audits

- Innovation Management Division will conduct monthly system inspections to ensure that users separated from the Department have had their accounts deactivated. System administrators no longer assigned to ITB will have their accounts deactivated appropriately.

- Audit Division conducts periodic inspections and audits of the ALPR system to ensure the Department adheres to existing policies and procedures.

This section was intentionally left blank

B. Whooster

Whooster is an investigative database and software platform that leverages search technology with publicly available information and private data sources (e.g., commercialized data brokers) to obtain information on persons of interest. This information includes names, phone numbers, addresses, and emails. End-users query this information for criminal investigations. Whooster is not limited to law enforcement and is available to private-sector enterprises.

The Department used two types of Whooster services:

- Whooster Web UI – Deployable from a computer (laptop) via a secure web-based login.
- Whooster SMS/TEXT – Deployable from a cellular telephone and requires no data usage.

Whooster is an investigative force multiplier that allows individuals to identify connections between persons of interest involved in criminal investigations and contact information. In addition, it is a resource used to help locate people based on what they self-report or self-register. Department investigators are tasked daily with locating individuals (e.g., suspects, victims, witnesses, and missing persons), identifying and apprehending suspects, and serving search warrants to services used or subscribed to by persons of interest. Whooster Web and SMS end-users query target-specific information on Whooster's secure platform. This critical "first step" provides investigators with the most current information.

Findings:

1. The Technology Met the Expectations of the Presentation to the Board of Police Commissioners and the Department when the Technology was Obtained

Whooster allows investigators to quickly and remotely query accurate and up-to-date information (e.g., people, addresses, telephone numbers, and vehicles) concerning active criminal investigations. It also aids investigators in locating missing persons and victims (e.g., kidnap for ransom cases). Investigators are afforded the technology and capability to conduct these inquiries to quickly further the respective criminal investigation.

Best practices dictate that information should not be from a sole source but corroborated by various sources. This technology allows investigators to manually cross-reference information received from Whooster's secure platform against other law enforcement systems already possessed and utilized by the Department. Once the information is obtained and vetted, investigators can seek further information from service providers via search warrants. This technology aligns and complies with the Department's current policies and procedures.

2. Frequency of Use

Two LAPD entities were identified as utilizing this technology in 2024. Those entities were Robbery-Homicide Division and South Bureau Homicide Division.

a. Robbery-Homicide Division (RHD) has used Whooster for crimes such as homicide (e.g., multiple murders, arson-related murder, murder involving police officers, and cold cases), robbery (e.g., robbery series, home invasion, and bank robbery), and kidnapping for ransom. On a regular basis, RHD personnel assist other LAPD entities in their criminal investigations. For 2024, RHD has conducted 7,568 queries using Whooster Web and 4,195 queries using Whooster SMS.

b. South Bureau Homicide Division (SBHD) has used Whooster primarily for murder investigations. In 2024, SBHD conducted 6,151 queries using Whooster SMS.

3. Efficacy of the Technology

This technology has been queried thousands of times during 2024 and has proven vital in quickly generating relevant investigative leads. These investigative leads have led to the successful identification, location, and apprehension of numerous felony suspects. Whooster has been utilized in a wide variety of criminal investigations.

Whooster is best known for its remote access, up-to-date addresses, and telephone data. It allows investigators to cross-check and cross-reference information obtained through Whooster against other technologies already used by the Department. Investigators have found this tool to be a valuable addition to other technologies. Also, best practices dictate that actionable information should not be derived from a sole source.

4. Personnel Compliance of All End-users

Whooster Web and Whooster SMS have been provided to a limited and select number of personnel with access to ongoing training, user manuals, and usage standards. Whooster is utilized during the course and scope of the end-user's assignment for criminal investigations following "right to know" and "need to know" standards.

Whooster's secure servers store all end-user activity, including the date and time of searches, content queried, and corresponding case numbers. The Department's search history information is not editable or removable from Whooster's platform. Whooster provides access to the Department's administrators to audit all search inquiries conducted by the assigned end-users. An annual inspection has been implemented to ensure all end-users comply with Department policies and procedures. The designated Administrators will conduct the inspection.

The respective lieutenant and commanding officer will review the inspection results. Further periodic and targeted inspections may be performed when appropriate.

5. The Cost of the Technology and Cost-Benefit Analysis

Breakdown of cost for Fiscal Year 2024/2025:

Robbery-Homicide Division - $33,000.00 (Whooster Web & Whooster SMS)

South Bureau Homicide Division - $4,506.00 (Whooster SMS)

This technology can be accessed remotely, enabling investigators to query new information at crime scenes. All the funding for this technology has been procured through various grants. The cost of this technology is significantly offset by the time it saves investigators gathering similar information via other resources. Ultimately, this saves the Department both time and expense by alleviating some of the travel time spent accessing similar information via a Departmental computer at a Departmental facility. This technology also lessens the amount of investigative hours because of the quick return of relevant results.

6. Identified Concerns and Proposed Mitigations

No concerns or proposed mitigations are indicated at this time.

Administrators have worked with and will continue to work with Whooster to identify, address, and resolve any concerns in the future (i.e., Federal or State law and Department policy changes).

7. Efficacy of the Existing Policy and Any Proposed Changes

Like other technologies/databases accessed by law enforcement, this technology follows the "right to know" and "need to know" standards. Administrators implemented the entry of criminal case numbers in conjunction with inquiries, which are later subject to audit or inspection.

The number of end-users is small, and personnel are selected based on their assignment and need for the technology. End-users are made aware of the designated administrator(s), that the system securely stores inquiries, and end-users' queries are later subject to audit.

8. Efficacy of the Training on the Existing Policy and Any Proposed Changes

Whooster provides training during the initial "onboarding" process and offers additional training, resources, and support on an ongoing basis. In addition, Whooster provides a user guide and offers weekly virtual training. This technology is straightforward to use and has a quick learning curve.

End-users are also made aware of their designated administrator(s). Administrators are primarily responsible for keeping end-users apprised of any relevant changes to the technology, policy, and usage.

Other Related Matters

Data Retention

All cases involving the query of information through Whooster are investigatory with a criminal predicate and legitimate law enforcement purposes. Data may be retained for ongoing investigations and criminal court proceedings. Data may be retained for long periods due to the length of an open investigation and the duration of court proceedings. This aligns with Department policy and procedures and all criminal court expectations, including discovery requirements, court proceedings, and appellate processes. Data no longer necessary for an investigation or court proceedings will be disposed of properly following Department procedures and criminal court expectations.

Data Security

All data is initially and exclusively held on Whooster's secure servers. The end-users can only access this information via the designated applications (Whooster Web and Whooster SMS). End-users cannot add any information to Whooster's platform, absent the addition of corresponding case numbers about searches conducted.

Investigators may retain information per standardized data retention periods (refer to data retention heading). Information retained is kept in accordance with current Department standards. Robbery-Homicide Division, SBHD, and the Internet Crimes Against Children Task Force all operate within secure facilities in areas with secondary levels of restricted access.

Whooster Web requires a password and Multi-Factor Authentication (MFA) to access the Whooster data. Computers used to access the Whooster Web application are password-protected. Whooster SMS is utilized on cellular telephones that adhere to the Department's cellular telephone policy (e.g., password-protected). Whooster SMS also requires an active account for every specific cellular telephone number. In addition, the designated cellular telephone number, which is authorized as having a Whooster account, must send an SMS message to a designated Whooster telephone number for any case number updates and inquiries.

Privacy, Civil Rights, and Civil Liberties (P/CRCL)

- Potential Impact on Privacy and Civil Rights

  Whooster is a commercially available application used by private and public sector entities. There are no identified negative impacts or foreseen infringements upon privacy and civil rights. Informational inquiries, conducted by end-users via Whooster's platform, involve investigatory cases with a criminal predicate. This is in accordance with Federal and State law and the Department's policies and procedures.

- Measures Currently in Place to Maintain Data Security

  Whooster data is stored on their secure servers. Investigators (end-users) maintain extracted and stored data per Department policies and procedures, along with any court case-mandated expectations. Devices that access and query the Whooster platform are secured via passwords (Whooster Web and SMS) and MFA (Whooster Web). Investigators are familiar with technical safeguards such as encryption and other digital/physical safeguard techniques. The Whooster system allows for an audit process, providing additional protection.

- Plan to Safeguard Privacy and Civil Rights

  The Department and the assigned end-users have existing best practices and standards to safeguard privacy, civil rights, and civil liberties (P/CRCL) in a balance with Operations Security (OPSEC). This includes administrators and technology coordinators who engage with vendors and personnel on P/CRCL matters. Available ongoing training between the vendor and end-user also aids in establishing this goal. Necessary and in-place protocols regarding the appropriate redaction of information concerning court cases eliminate the unnecessary and unwarranted public release of data. Given the balance of situational awareness and First Amendment-protected activity, right-to-release protocols ensure that all relevant factors are considered.

- Public Access to the Data

  While the Whooster platform is not publicly accessible without license agreements, the same raw data that Whooster collects and maintains is mostly available to the public via manual search techniques and processes. Reports and discoveries generated from Whooster may be confidential due to the investigated case, court proceedings, and sealing orders. The public who wishes to obtain Whooster collected information may submit a request for information to RMLAD, Discovery Section, in accordance with the CPRA and FOIA, as the law allows.

Inspections/Audits

An annual inspection has been implemented to ensure all end-users comply with Department policies and procedures. The annual inspection will be conducted by the designated Administrator(s). The respective lieutenant and commanding officer will review the inspection. In addition to the annual inspection, periodic and targeted inspections may be conducted on a case-by-case basis when necessary (Refer to Finding No. 4).

This section was intentionally left blank.

C. Skopenow

Skopenow is an analytical search engine that uses social media, deep web, and dark web data to facilitate an investigation into a person or business. Skopenow is not limited in its access to law enforcement; the platform is also available to private-sector enterprises.

Skopenow is an investigative force multiplier that aggregates and surfaces publicly available information. Due to the vast amount of information online (often spread across a wide variety of websites, applications, and other services), it takes investigators a considerable amount of time to search for, aggregate, and organize this information. Additionally, traditional search engines (such as Google) are not engineered for investigative purposes. Instead, they have business purposes, including displaying advertising. Skopenow, however, is designed to make content on the internet pertaining to the targeted and relevant search of an investigated person concerning a criminal case easier to decipher, document, and preserve in a discoverable format. Once located, this content may lead to additional avenues of investigation and legal process, including search warrants to service providers or additional avenues of inquiry. Skopenow also captures online content in a court-ready format, which saves considerable time.

Findings:

1. The Technology Met the Expectations of the Presentation to the Board of Police Commissioners and the Department when the Technology was Obtained

Skopenow is available to both public and private sector clients. Skopenow is a data processor that uses public data from across the internet to compile a digital analytical report for each target-specific search in conjunction with a criminal case. Skopenow is not a database; the digital reports are based on publicly available content. If public content is made private, Skopenow does not retain that information. Also, users of Skopenow do not contribute any data to the system. Skopenow replaces the laborious and time-consuming task of investigators "hand searching" the internet with a search engine that correlates relevant data into a report.

Skopenow has met the Department's expectations of fulfilling this task, saving many employee hours. It also quickly aggregates relevant data that can be reviewed, vetted, and used to further an active criminal investigation. All end-user searches comply with a "right to know" and "need to know" basis.

2. Frequency of Use

For 2024, RHD was identified as utilizing this technology. Robbery-Homicide Division routinely aids other Department entities in criminal investigations when RHD deems the request for the software's usage would apply to the criminal case.

This technology has been used for various cases and investigations, including but not limited to murder, attempted murder, kidnapping for ransom, and robbery. Robbery-Homicide Division has used Skopenow as an investigative force multiplier and has realized significant time savings. The usage level for the calendar year 2024 was approximately 412 queries. In comparison, the number of individual queries to separate databases and websites would be vastly larger if an end-user (investigator) had to query and amass the same amount of information gathered expediently by Skopenow.

3. Efficacy of the Technology

Skopenow has been utilized in a wide variety/type of criminal investigations and cases. This technology has been queried hundreds of times during the 2024 calendar year and has proven vital in quickly generating relevant investigative leads. These investigative leads have led to the successful identification, location, and apprehension of numerous felony suspects.

Investigators have found this tool to be an invaluable addition to other technologies. Skopenow is best known for its ability to quickly aggregate and analyze data and present it in a usable format. Also, best practices dictate that actionable information should not be derived from a sole source. Skopenow allows investigators to cross-check and cross-reference information obtained through Skopenow against other technologies already possessed by the Department.

4. Personnel Compliance of All End-Users

Skopenow allows the Department's administrator(s) to audit all search inquiries conducted by the assigned end-users. Skopenow's servers store all end-user activity, including, in part, the date/time of searches, content queried, and corresponding case numbers. The end-user cannot edit or remove any logged activity (search history) from Skopenow's server. Skopenow is assigned to a small number of investigators in assignments where the usage of this software is most applicable. Skopenow is utilized during the course and scope of the end-users' assignments for criminal investigations following "right to know" and "need to know" standards.

An annual audit has been implemented to ensure all end-users comply with Department policies and procedures. The annual audit is conducted by the designated administrator(s). The respective lieutenant and commanding officer review the audit. In addition, periodic and targeted audits may be performed when needed.

5. The Cost of the Technology and Cost-Benefit Analysis

Robbery-Homicide Division's cost for Fiscal Year 2024/2025 is $85,063.00.

The funding for this technology was procured through a grant. The cost of this technology is significantly offset by the time it saves investigators gathering similar

information via other resources, such as "hand searching" the internet. This technology can be accessed remotely, quickly enabling investigators to query fresh information at crime scenes. This fresh information is often very helpful in furthering an investigation in the early stages. It also aids in identifying suspects and victim accounts and a nexus between them, if any, allowing for the preservation of any data residing with service providers that the suspect may later remove. Skopenow also reduces the total number of employee work hours via the quick return of relevant results.

6. Identified Concerns and Proposed Mitigations

No concerns or proposed mitigations are appropriate. Administrators have worked with the vendor to make specific features available to bring this technology in line with Special Order No. 11, 2022, and current Department policies and procedures.

Administrators have worked with and will continue to work with Skopenow to find, address, and resolve any concerns in the future (e.g., Federal or State law and Department policy changes).

7. Efficacy of the Existing Policy and Any Proposed Changes

Like other technologies or databases accessed by law enforcement, this technology follows the "right to know" and "need to know" standards. The entry of criminal case numbers in conjunction with inquiries is mandatory and later subject to audit or inspection. The number of end-users is small, only 10, and personnel are chosen based on their assignment and need to use the technology. End-users are made aware of the designated administrators, that the system securely stores inquiries, and that the end-users' inquiries are later subject to audit.

8. Efficacy of the Training on the Existing Policy and Any Proposed Changes

Skopenow provides training during the initial "onboarding" process and offers additional training, resources, and support on an ongoing basis. Skopenow provides a user guide and offers virtual training. This technology is straightforward to use and has a short learning curve. End-users are made aware of their designated administrators. Administrators are primarily responsible for keeping end-users apprised of any relevant changes to the technology, policy, and usage.

Other Related Matters

Data Retention

All cases involving the query of information through Skopenow are investigatory with criminal predicate and legitimate law enforcement purposes. Data may be retained through ongoing investigations and criminal court proceedings. Data may be retained for long periods due to the length of an open investigation and court

- Plan to Safeguard Privacy and Civil Rights

  The Department and the assigned end-users have existing best practices and standards to safeguard privacy, civil rights, and civil liberties (P/CRCL) in a balance with OPSEC. This includes administrators and technology coordinators who engage with vendors and personnel on P/CRCL matters. Available and ongoing training between the vendor and end-user also aids in establishing this goal. Necessary and in-place protocols regarding the appropriate redaction of information concerning court cases eliminate the unnecessary and unwarranted public release of data. Given the balance of situational awareness and First Amendment-protected activity, right-to-release protocols ensure all relevant factors are considered.

- Public Access to the Data

  While the Skopenow platform itself is not publicly accessible, the same raw data Skopenow collects via its publicly available searches are available to the public via manual search techniques and processes. Reports and discovery generated from Skopenow may be confidential due to the investigated case, court proceedings, and sealing orders. The public may submit a request for information to RMLAD, Discovery Section, in accordance with the CPRA and FOIA, as the law allows.

Inspections/Audits

A 2024 annual audit was completed to ensure all end-users were compliant with Department policies and procedures per Special Order No. 11, 2022. The annual audit was conducted by the designated administrators. The respective lieutenant and commanding officer reviewed and approved the inspection. The methodology and results of the inspection are maintained at RHD and are available for inspection. In addition to the annual inspection, periodic and targeted audits may be conducted on a case-by-case basis when necessary (Refer to Finding No. 4).

This section was intentionally left blank.

D. Penlink Tangles (formerly known as Cobwebs Technologies)

Penlink (Tangles) is a web-based platform that searches for and analyzes open-source information (OSINT), publicly available information, and commercially available anonymized data. Searches using the technology are for criminal investigations and public safety threat assessments. Once the technology produces relevant results, they are filtered through and vetted by an investigator and/or crime analyst for their definitive relevance. Tangles makes products for both law enforcement and private-sector enterprises.

Findings:

1. The Technology Met the Expectations of the Presentation to the Board of Police Commissioners and the Department when the Technology was Obtained

Tangles allows users to analyze publicly available data effectively and efficiently in conjunction with criminal cases, critical incidents, and/or threats to public safety. Tangles is a force multiplier that replaces the laborious and time-consuming task of manually searching the internet for open-source information related to an investigation.

Tangles has met the Department's expectations of completing investigative tasks accurately and expeditiously, ultimately saving many human resource hours. With Tangles, searches are accomplished at an expedient rate with higher accuracy. Once the information is obtained and vetted, investigators can seek further information from service providers via search warrants. This technology aligns and complies with the Department's current policies and procedures. All end-user searches abide by the "right to know" and "need to know" basis.

2. Frequency of Use

The Department initially acquired Tangles on July 28, 2022. The Department purchased three concurrent licenses, 13 total users, which were divided between RHD and Major Crimes Division (MCD). Robbery-Homicide Division's investigative responsibilities include but are not limited to homicides (e.g., multiple murders, arson-related murder, murder involving police officers, and cold cases), robberies (e.g., robbery series, home invasion, and bank robbery), and kidnap for ransom. Major Crimes Division's investigative responsibilities include, but are not limited to, crimes related to threats to public safety (e.g., mass shootings, bomb threats, and serial arsons) and critical infrastructures. In addition to using the technology in their investigations, RHD and MCD personnel regularly use the technology to assist other Department entities with criminal investigations when necessary and appropriate. Tangles has been queried approximately 1,900 times during the calendar year 2024.

3. Efficacy of the Technology

Tangles has been queried approximately 1,900 times during the calendar year 2024 and has proven vital in quickly generating relevant investigative leads. Investigators can accurately and effectively sort open-source leads that have led to the utilization of other investigation techniques (e.g., search warrants, interviews, and forensic investigation). Results have included the successful identification, location, and apprehension of numerous felony suspects. Tangles have been utilized in a wide variety/type of criminal investigations and cases.

Investigators have found Tangles to be a valuable and complementary addition to other technologies already used by the Department. Additionally, Tangles allows investigators to cross-check and cross-reference obtained information against other Department technologies. This is significant as "best practices" dictate that actionable information should not be derived from a sole source.

4. Personnel Compliance of All End-Users

Tangles allow the Department's Administrator(s) to inspect all search inquiries conducted by the assigned end-users. Tangles' servers store all end-user activity, including, in part, the date/time of searches, content queried, and corresponding case numbers. The end-user cannot edit or remove any logged activity (search history) from Tangles' server. Tangles is assigned to a small number of investigators in assignments where the usage of this software is most applicable. Tangles is utilized during the course and scope of the end-users' assignments for criminal investigations following "right to know" and "need to know" standards.

An annual inspection has been implemented to ensure all end-users comply with Department policies and procedures. The designated administrators conduct the yearly inspection. The respective lieutenant and commanding officer review the inspection. In addition, periodic and targeted inspections may be performed when needed.

5. The Cost of the Technology and Cost-Benefit Analysis

Robbery-Homicide Division's cost for Fiscal Year 2024/2025 is $182,982.67.

The funding for this technology was procured through a grant. The cost of this technology is significantly offset by the time it saves investigators gathering similar information via other resources, such as "hand searching" the internet. This technology can be accessed remotely, quickly enabling investigators to query fresh information at crime scenes. This fresh information is often very helpful in furthering an investigation in the early stages. It also aids in identifying suspects and victim accounts and a nexus between them, if any, allowing for the preservation of any data residing with service providers that the suspect may later remove. Tangles also reduce the total number of employee work hours via the quick return of relevant results.

6. Identified Concerns and Proposed Mitigations

No concerns or proposed mitigations are appropriate. Administrators have worked with the vendor to make specific features available and to bring this technology in line with Special Order No. 11, 2022, and current Department policies and procedures.

Administrators have worked with and will continue to work with Tangles to find, address, and resolve any concerns in the future (e.g., Federal or State law and Department policy changes).

7. Efficacy of the Existing Policy and Any Proposed Changes

Like other technologies or databases accessed by law enforcement, this technology follows the "right to know" and "need to know" standards. The entry of criminal case numbers in conjunction with inquiries is mandatory and later subject to audit. The number of end-users is small, only six, and personnel are chosen based on their assignment and need to use the technology. End-users are made aware of the designated administrators, that the system securely stores inquiries, and that the end-users inquiries are later subject to audit.

8. Efficacy of the Training on the Existing Policy and Any Proposed Changes

Tangles provides training during the initial "onboarding" process and offers additional training, resources, and support on an ongoing basis. Tangles provides a user guide and offers virtual training. This technology is straightforward to use and has a short learning curve. End-users are made aware of their designated administrators. Administrators are primarily responsible for keeping end-users apprised of any relevant changes to the technology, policy, and usage.

Other Related Matters

Data Retention

All cases involving the query of information through Tangles are investigatory with criminal predicate and legitimate law enforcement purposes. Data may be retained with an ongoing investigation and criminal court proceedings. Data may be retained for long periods due to the length of an open investigation and court proceedings. This aligns with Department policy and procedures and all criminal court expectations, including discovery requirements, court proceedings, and the appellate processes. Data no longer necessary for an investigation or court proceedings will be disposed of properly following Department procedures and criminal court expectations.

Data Security

Investigators may retain information per standardized data retention periods (refer to data retention heading). Information retained will be kept per current Department standards. Robbery-Homicide Division operates within a secure facility with a secondary restricted access level. Personnel within the division are provided locking desks and have access to storage cabinets as an additional physical safeguard.

Computers used to access Tangles' web-based application/portal are password-protected desktop, laptop, or tablet computers. If a cellular telephone is utilized to access Tangles' platform, the Department's current cellular telephone policy (e.g., password-protected) is adhered to.

Privacy, Civil Rights, and Civil Liberties (P/CRCL)

- Potential Impact on Privacy and Civil Rights

  There are no identified negative impacts or foreseen infringements upon privacy and civil rights. Informational inquiries, conducted by end-users via Tangles' platform, involve investigatory cases with a criminal predicate. This is in accordance with Federal law, State law, and the Department's policies and procedures.

- Measures Currently in Place to Maintain Data Security

  Tangles does not retain a database. Investigators (end-users) maintain any extracted and stored data following Department policies and procedures, along with any court case-mandated expectations. Devices used to access and query the Tangles platform are secured via passwords. Facilities in which these (printed) records would be stored are secured and inaccessible to unauthorized law enforcement/public. Most investigators are familiar with technical safeguards such as encryption and other digital/physical safeguard techniques. The Tangles platform allows for an audit process, which is in place, creating additional protection.

- Plan to Safeguard Privacy and Civil Rights

  The Department and the assigned end-users have existing best practices and standards to safeguard privacy, civil rights, and civil liberties (P/CRCL) in balance with OPSEC. This includes administrators and technology coordinators who engage with vendors and personnel on P/CRCL matters. Available and ongoing training between the vendor and end-user also aids in establishing this goal. Necessary and in-place protocols regarding the appropriate redaction of information concerning court cases eliminate the unnecessary and unwarranted public release of data. Given the balance of situational awareness and First Amendment-protected activity, right-to-release protocols ensure all relevant factors are considered.

- Public Access to the Data

  While the Tangles platform itself is not publicly accessible, the same raw data Tangles collects via its publicly available searches are available to the public via manual search techniques and processes. Reports and discovery generated from Tangles may be confidential due to the investigated case, court proceedings, and sealing orders. The public may submit a request for information to Risk Management and Legal Affairs Division, Discovery Section, in accordance with the CPRA and FOIA, as the law allows.

Inspections/Audits

A 2024 annual audit was completed to ensure all end-users were compliant with Department policies and procedures per Special Order No. 11. The annual inspection was conducted by the designated administrators. The respective lieutenant and commanding officer reviewed and approved the audit. The methodology and results of the audit are maintained at RHD and are available for inspection. In addition to the annual inspection, periodic and targeted inspections may be conducted on a case-by-case basis when necessary (Refer to Finding No. 4).