**DRAFT for PAB Consideration**

MEMORANDUM

DATE: February 27, 2024
FROM: City of San Diego Privacy Advisory Board (PAB)
TO: The Honorable Council President Elo-Rivera and Members of the San Diego City Council
RE: San Diego Police Department's (SDPD) Use Policy for Grayshift GrayKey

## I. RECOMMENDATION

**The PAB recommends that the City Council approve the proposal with modifications as indicated below.**

## II. RECOMMENDED MODIFICATIONS

On February 15, 2024, SDPD provided written responses to PAB questions and answered follow-up questions about this technology ("SDPD Response"). The PAB recommends that content from these answers be incorporated into the Use Policy and Surveillance Impact Report to provide the City and the public additional details. Below we provide more detailed guidance, extracting information from the SDPD Response and providing recommendations about placement of information in the current Use Policy.

A. DEPARTMENT MANUAL: As with all other technologies, the PAB recommends that relevant sections of Department Manuals and Procedures be included directly in the Use Policy or incorporated by reference. The TRUST Ordinance requires that pertinent information be included in the Use Policy itself, not in other documents that are not reviewed by the PAB, public, and City Council. The practice of referencing, without incorporating, a particular manual or procedure causes confusion for the public and does not allow for review of changes to the uses and access procedures, as required by the TRUST Ordinance.

   In this Use Policy, for example, there is a reference to "Forensic Technology Unit Manual Version 05.22.2022," a document that is not readily available through an Internet search.

B. ALL SECTIONS: The Use Policy should be modified in relevant sections to use limited lists. Currently, the Policy uses open language (*e.g.*, "when proper authority, *such as* a search warrant or consent"). This indicates that there may be other, unlisted examples. To the maximum extent possible, the Use Policy should have exclusive lists.

C. USE:
   1. This section should be updated to use exclusive language. Otherwise, this indicates that there are other uses that are not listed. If there are other uses, SDPD should list those. Prohibited uses should also be stated.
   2. The use section should be modified to incorporate information from the SDPD Response explaining that, while there is no way to limit what is extracted from a

cellular device, the requesting investigator's review of the resulting report will be limited to the original authorization (warrant or consent).

D. DATA ACCESS: The Use Policy should be modified to provide concrete information about access to the data and results, not merely access to the software. The following, from the SDPD Response, should be added: The following SDPD personnel have access to the results of an extraction:
   - The SDPD Crime Laboratory's Forensic Technology Unit (FTU) – FTU criminalists are the administrators of the mobile device extraction network,
   - The officer/detective/FTU criminalist who conducted the device extraction,
   - The requesting investigator, and
   - IT/Data Systems analysts who oversee network security and management.

   In addition, the Use Policy should be modified to include a statement that access to resulting reports will only be authorized when directly relevant to an ongoing investigation.

E. DATA RETENTION: Because the Grayshift GrayKey technology does not allow for limited extractions (*i.e.*, extractions from mobile devices are "all or nothing"), the retention section should be modified to specify how long information that is unrelated and irrelevant to the investigation will be maintained.

F. TRAINING: The Use Policy should be modified to include the specific trainings outlined in the SDPD Response in addition to training on the Policy itself.

G. AUDITING AND OVERSIGHT:
   1. The Use Policy should be modified to provide information about who does audits of SDPD uses of this technology and who has oversight of uses. The current document does not specify any auditing requirements except for logging of access.
   2. The following modification is recommended: "Misuse of the system, data, or resulting reports ~~would~~ must be reported to and investigated by the Department's Internal Affairs unit."

For the above stated reasons, the Privacy Advisory Board respectfully recommends that the City Council **approve the proposal** with the recommendations above.

Cc: SDPD Chief Nisleit
CPT Jim Jordon
LT. Eric Portnoy
Chloe Madison