The City of San Diego

Staff Report

DATE ISSUED:	November 6, 2023	
TO:	Privacy Advisory Board	
FROM:	San Diego Police Department (SDPD)	
SUBJECT:	Presentation of Use Policies and Surveillance Impact Reports Associated with PENLiNK PLX Software	
Primary Contact:	Captain Matt Novak	Phone: (619) 531-2339
Secondary Contact:	Lieutenant Michael Swanson	Phone: (619) 531-2563
Council District(s):	Citywide	

OVERVIEW:

On August 10, 2022, the City of San Diego amended and added Chapter 2, Article 10, of the San Diego Municipal Code – the "Transparent and Responsible Use of Surveillance Technology" (Surveillance Ordinance). The Surveillance ordinance is designed to provide greater transparency to the City Council and the public when the City uses or acquires any technology that meets the City's definition of surveillance. The Surveillance Ordinance requires that for each technology that meets the criteria for surveillance, City Departments must:

- Hold at least one or more community meetings in each City Council district where the proposed surveillance technology is deployed, with an opportunity for public comment and written response.
- Prepare a Surveillance Use Policy that includes the purpose, use, data collection, data access, data protection, data retention, public access, third-party data sharing, training, auditing, oversight, and maintenance.
- Prepare a Surveillance Impact Report including description, purpose, location, impact assessment, mitigations, data types and sources, data security, fiscal cost, third-party dependence, alternatives, track record, public engagement, and comments.
- Present the item to the Privacy Advisory Board for review.
- Present the item to the City Council for the acquisition and deployment of all new and currently used surveillance technologies.
- Provide annual reports on surveillance technology use, impact, and acquisitions.

PROPOSED ACTIONS:

In accordance with the Board Notification and Review Requirements outlined in section 210.0102 of the Surveillance Ordinance, the San Diego Police Department (SDPD) is requesting approval for the use, funding, acquisition, and sharing of technology that falls within the definition of surveillance technology under the ordinance. Specifically, the item being requested is known as PENLiNK PLX software (PENLiNK PLX).

DISCUSSION OF ITEM:

SDPD's mission is to provide the highest quality police services to the communities it serves. SDPD values transparency, and public input and welcomes open dialogue about its practices and operations. The preservation and sustainability of public safety, officer safety, and civil rights are paramount. SDPD further recognizes the importance and value of public disclosure regarding the qualified surveillance technology we use. We intend to present to the Privacy Advisory Board our use of PENLiNK PLX.

SDPD's lead, the Internet Crimes Against Children Task Force (SDICAC) is one of a national network of sixty-one coordinated task forces, representing over 5,400 federal, state, and local law enforcement agencies, dedicated to investigating, prosecuting, and developing effective responses to internet crimes against children. SDICAC is composed of thirty-three law enforcement agencies and four prosecutorial bodies spanning three counties: San Diego, Riverside, and Imperial Valley. As the lead agency of the task force, the Commander, a San Diego Police Department Detective Sergeant, is responsible for providing and procuring technology/equipment, training, and travel to each member of the task force, ensuring each agency/investigator/prosecutor is capable of executing their duties to proactively and reactively protect children from online predators. SDICAC is funded primarily through grant funding awarded by the Department of Justice, Office of Juvenile Justice and Delinquency Program. Additional grant funding is provided by the California Governor's Office of Emergency Services (CalOES).

PENLiNK PLX is computer software available to local, state, federal, and international law enforcement agencies. As defined on PENLINK.com, the software provides, "digital investigative solutions bringing innovative analytical capabilities to reveal connections and gain insights more quickly. Combat job fatigue and burnout with PLX and its powerful, easy-to-use, and flexible array of reporting and analytical tools to help reveal connections, trends, and relationships that might otherwise go undetected. With options for interactive grids, graphical analysis, and reporting across phone calls, messaging, social media, and more, PLX does in minutes what would take investigator weeks to do manually." PENLiNK PLX provides ICAC members the ability to examine large data sets obtained through search warrants in one integrated view. The program parses out information such as imagery, text, chat, email, and documents, and organizes it in a manner that is useable and logical allowing task force members to more efficiently review, oftentimes, terabytes of information. It is used to support SDICAC criminal investigations.

PENLiNK PLX, using proprietary software coding, parses out the data identified in the authored and granted search warrant into usable, logical files (e.g., images, videos, emails, and text messages). Investigators then review the organized data and determine the evidentiary value of what was extracted/received. When the review is complete, PENLiNK PLX will produce a report indicating the items selected. SDICAC members validate the authenticity of the information through the

appropriate custodian of records through the service of either search warrants or subpoenas. That report is then provided to the prosecutor as part of a much larger investigation.

PENLiNK PLX is stored and maintained in SDICAC, a secured office located away from SDPD Headquarters. Only authorized users have access to the office space and technology. PENLiNK PLX is not located on any SDPD network computer and can only be accessed by logging in to the computer with the software installed at SDICAC. The computer has no internet access and is not accessible by the vendor. Additionally, the software can only be installed through a specific process, it cannot be moved, and the user must be an authorized user with a valid software license. PENLiNK PLX cannot be accessed outside of the SDICAC.

Data retained is limited to the files selected by the task force member to be downloaded into their digital case file located on the ICAC Network Attached Storage (NAS) system located in the secured ICAC office.
When a task force member determines that downloaded PENLiNK PLX information no longer has a legitimate law enforcement use, the information is destroyed in a manner so that the identity of the subject can no longer be reasonably ascertained, e.g., shredding printouts, deleting electronic records & clearing from trash folders.

Computers, smartphones, and tablets are used to commit crimes, including crimes against children, and, thanks to the science of digital evidence forensics, SDICAC uses technology to fight crime, protect children, and obtain the evidence necessary to prosecute those victimizing children online.

Digital evidence is information stored or transmitted in binary form that may be relied on in court. It can be found on a computer hard drive, a smartphone phone, a tablet, on loose digital media, in cloud account files, and on social media platforms. Digital evidence is commonly associated with the online exploitation and enticement of children. Digital evidence can be used to prosecute all types of online crimes perpetrated against children. For example, a suspect's e-mail, image files, chat logs, other phone files, data contained within a cloud account, or data retained by electronic service providers might contain critical evidence regarding their intent, their whereabouts at the time of a crime, and their relationship with the victim and/or other suspects. In 2022, SDICAC conducted 4271 investigations. As a result of those investigations, 1771 digital storage devices, including smartphones and tablets, were forensically examined after proper legal authority was granted. Those examinations resulted in the arrest and prosecution of more than 128 persons who were victimizing children online.

In an effort to fight the online exploitation and enticement of children and to collect relevant digital evidence, SDICAC incorporates the collection and analysis of digital evidence, also known as digital forensics, into its infrastructure. SDICAC, as with all law enforcement agencies, is challenged by the ever-growing world of online predators and is constantly seeking the most effective means to collect

and analyze digital evidence, such as PENLiNK PLX, keeping up with rapidly evolving technologies such as smartphones and tablets.

The materials required under the Surveillance Ordinance accompany this Staff Report in compliance with the ordinance to provide information surrounding the proposed use of PENLiNK PLX and answer the many questions associated with their use and community impact.

David Nisleit

Chief of Police