

This is the text of a Penlink statement sent via email to CPJ on July 3, 2026, responding to questions about Citizen Lab's April 2026 [report](#) on Penlink's Webloc product, the risks of Penlink's products being used to target journalists, and Penlink products' usage of data from software development kits and real-time bidding systems:

Committee to Protect Journalists (CPJ),

Thank you for your inquiry related to the report published by The Citizen Lab. We appreciate the opportunity to provide our response and clarify several points raised in the publication. We want to emphasize that this report contains significant inaccuracies and mischaracterizations of Penlink's current platforms, operations, and customer relationships.

We also want to emphasize that Penlink and our employees appreciate and understand the vital role journalists play in this country and around the world. Like all people, journalists deserve to be treated with respect and dignity, and we are committed to protecting populations from mistreatment through the use of our products.

We have established safeguards to reduce the likelihood that our technologies may be used in ways that are incompatible with applicable legal, regulatory, or ethical frameworks. This includes vetting potential customers outside of the U.S. and refusing to work with countries or organizations with a history of disregard for civil liberties. As part of that process, we often consult resources such as Freedom House to inform our analysis, which explicitly addresses freedom of expression.

Our License Agreement prohibits the use of Penlink products, including Tangles and Webloc, to abuse internationally recognized human rights. Targeting journalists is recognized as a serious violation of human rights under both international humanitarian law (IHL) and international human rights law (IHRL).

In the U.S., our federal, state, and local law enforcement customers are required to act legally and use our technology within the bounds of their authority. They are required to follow their respective legal requirements and internal procedures, including determining which services to purchase and how they use the tools. We are committed to operating responsibly under all applicable laws and regulations, as our customers are required to do.

We understand the sensitivity and complexity of data privacy and operate under thoughtful compliance, due diligence, and responsible-use standards. We operate within established compliance frameworks, including ISO, SOC, NIST, CJIS, CMMC, and CSA, supported by independent audits, government programs, and industry-recognized best practices.

Our solutions do not enable users to identify or target individuals or groups based on protected characteristics, occupations, affiliations, or attendance at specific sensitive locations, such as schools or hospitals. Location data is obtained from providers who obtain user consent for

location data sharing through SDKs and who filter out sensitive locations from their datasets, consistent with FTC mandates.

Penlink is a trusted software provider for law enforcement and public safety agencies, delivering mission-critical digital intelligence to help save lives and bring justice. Our customers use these solutions to locate kidnapped children, combat human and drug trafficking, and identify potential terror threats, among other critical uses.

Please attribute this statement to a Penlink Spokesperson.