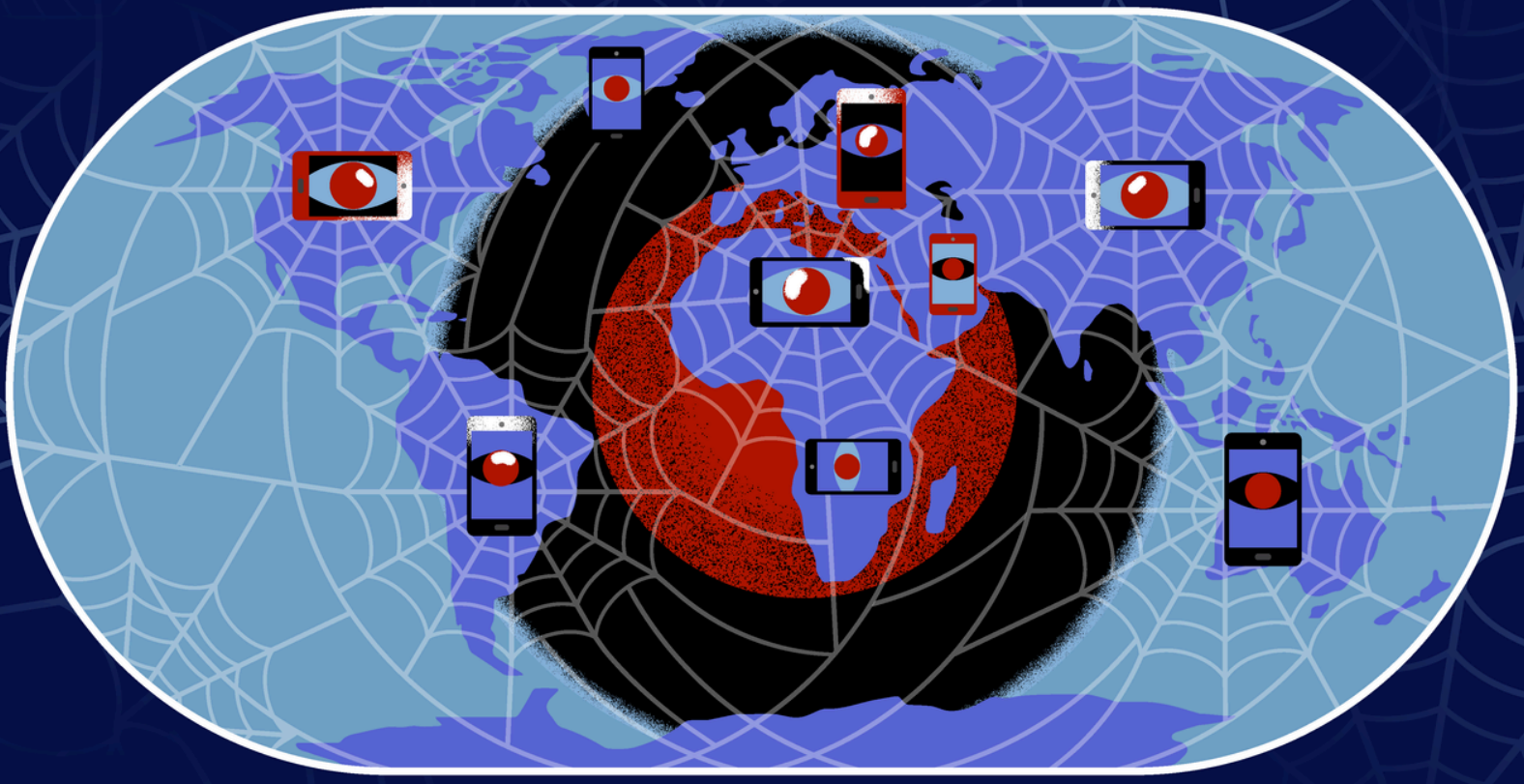
UNCOVERING WEBLOC

An Analysis of Penlink's Ad-based Geolocation Surveillance Tech



April 9, 2026

Report No. 191

By Wolfie Christl, Astrid Perry, Luis Fernando Garcia, Siena Anstis, and Ron Deibert

THECITIZENLAB

munk school OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

Copyright

Suggested Citation

Wolfie Christl, Astrid Perry, Luis Fernando Garcia, Siena Anstis, and Ron Deibert. “Uncovering Webloc: An Analysis of Penlink’s Ad-based Geolocation Surveillance,” Citizen Lab Report No. 191, University of Toronto, April 9, 2026.

Acknowledgements

We would like to thank Alberto Fittarelli, Rebekah Brown,and John Scott-Railton for reviewing this report. Special thanks to Alyson Bruce, Anna Mackay, Claire Posno, and Adam Senft for editorial and graphics support.

Special thanks to Donncha Ó Cearbhaill and Amnesty Tech for providing us with information about Cobweb's infrastructure.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is a world-renowned research unit led by Professor Ronald J. Deibert at the University of Toronto's Munk School of Global Affairs & Public Policy. We investigate novel threats to democracy, human rights, and global security in the digital ecosystem. Over the past 25 years, the Citizen Lab's evidence-based research has played a critical role in demonstrating how digital technologies are used to undermine human rights. The Citizen Lab has published more than 180 evidence-based, peer-reviewed research reports, available online.

Contents

Excerpt

Location data collected from mobile apps and digital advertising can reveal habits, interests and almost any other aspect of someone's life. In this report, we uncover how a geolocation surveillance system called Webloc uses ad-based data to monitor hundreds of millions of people across the globe.

Key Findings

- Webloc is a global geolocation surveillance system that monitors hundreds of millions of people based on data purchased from consumer apps and digital advertising. It was developed by Cobwebs Technologies and is now sold by its successor Penlink.
- In collaboration with the European investigative journalism platform *VSquare*, we reveal that Hungarian domestic intelligence has been using Webloc since at least 2022 and continues to use it as of today. Webloc customers also include the national police in El Salvador.
- U.S. customers include ICE, the U.S. military, Texas Department of Public Safety, DHS West Virginia, NYC district attorneys, and several police departments in Los Angeles, Dallas, Baltimore, Tucson, Durham and in smaller cities and counties like City of Elk Grove and Pinal County.
- Based on the responses to 96 freedom of information requests we conclude that governments in Europe and the U.K. are highly nontransparent about their potential use of ad-based surveillance.
- Cobwebs Technologies has links to the spyware vendor Quadream through Cobwebs Technologies founder Omri Timianker, who now oversees the international operations of Penlink.
- Webloc is sold as an add-on product to the social media and web intelligence system Tangles. Based on technical analysis and other sources we show that Tangles and other products developed by Cobwebs Technologies are used in many countries across the globe.
- We briefly investigate another Cobwebs product named Trapdoor that appears to help trick victims into revealing information. Our analysis leads us to believe that Trapdoor can help facilitate the deployment of malware on devices.

Introduction

Targeted and mass surveillance based on everyday consumer data from mobile apps and digital advertising has been referred to as advertising intelligence (ADINT). We refer to it as "ad-based surveillance technologies." These technologies have proliferated alongside the personal data surveillance economy. They are poorly regulated and often sold by firms that operate without transparency, raising serious security, privacy, and civil liberties concerns – especially when used by authoritarian governments that lack proper oversight.

In this report, we investigate, summarize and document what we know about the ad-based geolocation surveillance system Webloc. Developed by Cobwebs Technologies, Webloc is now sold by Penlink, after the companies merged in 2023.

Webloc has recently sparked significant public debate as the U.S. Immigration and Customs Enforcement (ICE) entered into a contract which allows it to access data on hundreds of millions of people for surveillance purposes. In March 2026, 72 senators and representatives in the U.S. Congress called for an investigation into "warrantless purchases of Americans' location data" by ICE and other U.S. agencies.

Based on documents related to contracts and other sources, we analyze in detail the capabilities provided by Webloc, which is sold as an add-on product to the widely used social media and web intelligence system Tangles. According to the documents we have seen, Webloc provides access to a constantly updated stream of records from up to 500 million mobile devices across the globe that contain device identifiers, location coordinates, and profile data harvested from mobile apps and digital advertising. Customers can monitor the location, movements, and personal characteristics of entire populations up to three years in the past. As discussed in **Section 3**, our analysis of Webloc's capabilities is based on a number of documents from 2021, 2022, 2023, and 2025.

Our research shows that intrusive and legally questionable ad-based surveillance (i.e. without a warrant or adequate oversight) is being used by military, intelligence, and law enforcement agencies down to local police units in several countries across the globe.

Webloc Customers: Hungary, El Salvador, and the United States

In collaboration with Hungarian journalist Szabolcs Panyi, who is publishing a parallel report via the European investigative platform *VSquare,* we reveal that domestic intelligence in Hungary has been using Webloc since at least 2022 and continues to use it as of today. **This represents the first confirmation of the use of ad-based surveillance technology in Europe.**

Based on a systematic analysis of media reporting, public records, and other sources, we show that El Salvador National Civil Police purchased Webloc in 2021. These sources also show that Webloc customers in the U.S. include the U.S. military, ICE, West Virginia Department of Homeland Security, Texas Department of Public Safety, NYC district attorneys, and police departments, both large and small, in Los Angeles, Dallas, Baltimore, Durham, Tucson, Pinal County and City of Elk Grove.

Potential Customers

In Europe and the U.K., we sent 96 freedom of information (FOI) requests to law enforcement agencies and local police departments in 14 countries and to six European Union bodies. Many were rejected or received no response. Europol confirmed to hold information relating to Webloc but refused to disclose it. The U.K.'s Home Office and the Swedish Police Authority would neither confirm nor deny information

requests relating to Webloc while stating they did not have access to products from similar vendors. Austrian, Dutch, and Romanian ministries refused to say whether they use Webloc. While five U.K. police departments confirmed to not hold information on Webloc, 39 would neither confirm nor deny.

We further examined potential Webloc customers in additional countries. The local police in Venice, Italy hosted a Webloc training event in 2022. Israeli military personnel received Webloc training while working for the Israel Defense Forces. A Dutch reseller promotes Webloc to European customers. Based on our technical analysis and other sources reviewed for this report, we believe that further research would be fruitful with respect to potential Webloc purchases in the Netherlands, Mexico, Vietnam, and Singapore. The maps shown in documents that describe Webloc indicate that it was used to track people in Germany, Austria, Italy, Hungary, Romania, United Arab Emirates, Israel, Singapore, and Russia.

Server Infrastructure

Based on technical analysis, we mapped out server infrastructure that we attribute to deployments of Tangles, Webloc or other products developed by Cobwebs Technologies. The analysis shows that servers affiliated with Cobwebs Technologies are located in many countries including in the U.S., U.K., Israel, Netherlands, Germany, Sweden, Norway, Italy, France, Ireland, Hungary, Poland, Cyprus, Mexico, Colombia, Brazil, Australia, Japan, Singapore, Hong Kong, India, Indonesia, United Arab Emirates, Iraq, and Kenya. We do not know whether the server locations represent customers located in these countries.

Corporate Analysis

Analysis of corporate records and other public information indicates that Cobwebs Technologies is linked to the spyware vendor Quadream. Omri Timianker, the founder and former president of Cobwebs Technologies who now oversees Penlink's international operations, holds an indirect interest[1] in Quadream. A former key executive and investor in Cobwebs Technologies is a key investor in Quadream. The Citizen Lab previously revealed that Quadream's spyware was used to target civil society, journalists and political opposition figures. Quadream was reportedly trying to sell its assets in 2023, but it is unclear whether they have and its Israeli corporate entity is still operational.

Cobwebs' Products

We briefly investigate other products developed by Cobwebs Technologies. Lynx, a system that helps facilitate undercover operations on the web and manage fake accounts on social media platforms, was used in the U.S. and El Salvador, as suggested by public records and media reports. Another system named Trapdoor, promoted by Cobwebs Technologies as an "active web intelligence" solution, has rarely been reported anywhere. A "technical specifications" document refers to Trapdoor as a "social engineering platform." The document and technical analysis suggest that Trapdoor is or was a system

[1] The founder and long-term president of Cobwebs Technologies holds an indirect interest in Quadream through a chain of corporate ownership and partnership arrangements as shown in Figure 14.

that helps customers create fake web pages and send phishing links to victims in order to trick them into revealing information. Our analysis further suggests that Trapdoor can help facilitate the deployment of malware on a victim's device. Based on technical analysis, we identified potential Trapdoor servers located in Kenya, Indonesia, Singapore, Hong Kong, U.A.E., and Japan. We do not know whether Lynx and Trapdoor are still being sold by Penlink. In its response to the Citizen Lab, Penlink claims, without being specific, that our report describes "products that no longer exist."

The U.S. Department of Homeland Security (DHS) used Tangles to compile dossiers on protesters, according to an internal DHS report, as discussed in **Section 2**. Meta mentioned Cobwebs Technologies prominently in its 2021 "Threat Report on the Surveillance-for-Hire Industry," banning it from its platform. Meta observed accounts used by Cobwebs customers engaging in social engineering and tricking people into revealing information including "frequent targeting of activists, opposition politicians and government officials." Cobwebs Technologies stated the report was false.

Methodology

We adopted a multi-method research design for this report. We conducted a comprehensive desk-based review of online sources (both current and historical), including media reporting, marketing materials, contracts, and publicly available procurement records. For our corporate mapping research, we obtained corporate filings from official company registries.

To ascertain which governments in Europe have had access to Webloc, or currently have access, we sent 96 freedom of information (FOI) requests across Europe. Our FOIs spanned 14 countries and six European Union bodies. For the most part, we sent these requests to agencies responsible for immigration and law enforcement. We also appealed several refusals by government agencies to provide information in response to our FOIs.

We also worked in collaboration with Szabolcs Panyi, a Hungarian journalist, to confirm the sale of Webloc to the Hungarian government. Mr Panyi relied on primary documents shared with him and several anonymous sources with ties to the Hungarian intelligence industry to confirm his findings. We independently reviewed a partial selection of these documents.

We also performed technical research by using browser testing on publicly available web resources and common DNS, IP and URL telemetry tools. We mapped out the server infrastructure we consider to be associated with Cobwebs Technologies and products developed by the company.

1. Background

In February 2020, an investigation by Byron Tau published in the Wall Street Journal confirmed for the very first time that U.S. government agencies purchase commercial smartphone data that maps the movements of millions for surveillance purposes. His article revealed that ICE bought access to location data from a digital marketing firm that obtained it from ordinary consumer apps, such as games or weather apps, to track immigrants.

Since then, investigations by journalists, researchers, and policymakers have shown that many government agencies in the U.S. have bought data on the behaviours, personal characteristics, and locations of hundreds of millions of people gathered from mobile apps and digital advertising firms. This includes a U.S. military unit that conducts drone strikes, an intelligence agency that used it for domestic surveillance without a warrant, and federal, state and local law enforcement.

Targeted and mass surveillance based on commercial data from mobile apps and digital advertising has been referred to as "advertising intelligence" (ADINT), a term that was reportedly coined by the surveillance industry itself. We refer to it as "ad-based surveillance technologies." While the public has learned a lot about ad-based surveillance vendors and their customers in the U.S. in recent years, as well as about vendors in other regions, little is known about how ad-based surveillance is used across the world in regions other than the U.S.

Mobile App and Digital Advertising Data

Ad-based surveillance vendors and their customers typically obtain mobile app and digital advertising data either from SDK-based or RTB-based sources, as confirmed by U.S. government records.

RTB-Based Data Sources

RTB-based data sources access data streams from the real-time bidding (RTB) system in digital advertising. Every time a person uses a mobile app or website that displays ads, an auction determines what ad they see. During that auction, which occurs within less than a second, their user data (described in more detail below) is shared with dozens or hundreds of digital marketing firms who participate in the bidding process. As the data is broadcasted without any security measures, surveillance vendors access it either by buying it from data brokers or by participating in the ad auctions themselves. An average European citizen's data is broadcasted to an unknown number of parties a few hundred times a day.[2]

[2] Two reports "Europe's Hidden Security Crisis" and "America's Hidden Security Crisis" by Johnny Ryan and Wolfie Christl, Irish Council for Civil Liberties (ICCL), 2023. Available at: https://crackedlabs.org/en/rtb-security-crisis

SDK-Based Data Sources

SDK-based data sources access data via third-party tracking software embedded in mobile apps. Many apps installed on Android and iOS phones, whether a game or a dating app, contain tracking software from one or several third parties. App vendors embed third-party software into their apps because they want to add functionality, analyze their users, benefit from displaying ads or simply sell user data. This third-party software is often integrated into an app in the format of a so-called software development kit (SDK). Surveillance vendors typically access the data by buying it from data brokers who directly or indirectly operate third-party software embedded in apps.[3]

Raw Data

The raw data collected from both types of sources typically consists of a device identifier, a timestamp, and other attributes that describe a person's behaviour or characteristics, such as their current geolocation, the app used at the time of collection and information about their device, operating system, and language. RTB-based data sources can provide additional attributes such as a person's age, gender, interests, habits, and purchases, which are used for ad targeting. SDK-based data sources can potentially access all data that the mobile app they are embedded into can access. This can include in-app behaviour, data on nearby Wi-Fi access points and Bluetooth devices, or even data from sensors such as the gyroscope, which measures how a phone is being held and moved.

Device Identifiers

Device identifiers are essential to track, follow, and profile people both in digital marketing and in ad-based surveillance. Data collected from both RTB- and SDK-based sources contains so-called Mobile Advertising IDs (MAIDs), which identify a phone or other mobile device and the person using it. While the advertising industry has long argued that Advertising IDs were 'anonymous', they are widely used to track, follow, and profile people both in digital marketing and by surveillance vendors who sell to governments.

The U.S. Federal Trade Commission recently clarified that Advertising IDs "offer no anonymity in the marketplace," because "many" businesses "regularly link consumers' MAIDs to other information about them, such as names, addresses, and phone numbers." As both RTB-based and SDK-based surveillance rely on Advertising IDs or other identifiers used in digital marketing, we refer to both as ad-based surveillance. Both may also utilize the IP address of the user for identification purposes.

Ad-Based Mass Surveillance

One data broker who obtained RTB-based data and sold that data to U.S. federal government customers via defense contractors claimed to have data on more than 1 billion mobile devices. Another one

[3] Out of Control. How consumers are exploited by the online advertising industry. A report by the Norwegian Consumer Council, 2020. Available online: https://storage02.forbrukerradet.no/media/2020/01/2020-01-14-out-of-control-final-version.pdf

collected RTB-based data from thousands of apps. Data brokers that obtain SDK-based data typically collect data on a lower number of people. One company who sold to the U.S. military via another firm claimed to collect data from 40 million phones via its SDK embedded in 400 apps, including Muslim prayer and family safety apps. A recent document referring to ICE's purchase of the geolocation surveillance system Webloc discusses "billions of daily location signals from hundreds of millions of mobile devices."

Geolocation Tracking and Restrictions to Data Access

The types of data that can be obtained from a phone depend on the apps installed on the device, the data those apps can access, and the permissions granted by the user. This specifically applies to geolocation tracking, which represents a major use case for ad-based surveillance. Apple's App Tracking Transparency (ATT) initiative, and to a much lesser extent, Google's improvements in Android permissions, have restrained access to geolocation data. To circumvent those restrictions, data collection efforts focus on apps that require access to location data such as weather, navigation, fitness, and dating apps.

When the exact GPS location of a user is unavailable, data brokers infer the approximate location at the city level from the user's IP address. SDK-based data may also contain location records inferred from data on Wi-Fi access points nearby a mobile device. Another obstacle lies in the fact that much of the data harvested and traded for digital marketing purposes is inaccurate. This is specifically true for geolocation data, as confirmed by the industry itself. For targeted surveillance, however, it does not matter whether 90% of the data is flawed, as long as the target's device identifier is in the set.

Implications for Rights, Lawfulness

Location data and similar data collected from apps and digital advertising are highly sensitive. They can reveal information about a person's home, workplace, family, friends, religion, political views, sexual orientation or health issues. The systematic misuse of data on hundreds of millions of people covertly purchased from everyday consumer apps and digital advertising for warrantless surveillance raises serious concerns about civil liberties and fundamental rights. In the U.S. and in Europe, both the lawfulness of governments using ad-based data for surveillance and the lawfulness of sharing the data over the entire supply chain, from apps and advertising firms to data brokers and surveillance vendors, are highly controversial, as discussed in **Section 10**.

2. Cobwebs, Penlink and Their Products

The ad-based surveillance system Webloc was initially developed by the Israeli company Cobwebs Technologies, which has been selling a range of surveillance technology solutions to national security organizations, law enforcement agencies, and commercial clients. Founded in 2015 by former members of Israeli special forces and intelligence units, Cobwebs Technologies was acquired by the U.S. investment firm Spire Capital in 2023 and merged with Penlink, a U.S.-based surveillance technology

vendor also owned by Spire Capital. The three founders of Cobwebs Technologies have since taken over key executive roles at Penlink, leading its technology, product, marketing, strategy, and international sales initiatives.

According to corporate records, Cobwebs Technologies has operated corporate entities in Israel, U.S., U.K., Germany, Singapore, and New Zealand.[4] A 2021 version of its website also listed offices in Mexico, Indonesia, and India. After it became part of Penlink in 2023, the Israeli, U.K. and German entities were renamed to contain the term "Penlink" or "Pen-link" instead of "Cobwebs."[5] Several products developed by Cobwebs Technologies are now sold by Penlink.

Cobwebs Technologies' product portfolio has been centred around its web and social media investigation platform Tangles, accompanied by additional products for mobile location surveillance, financial intelligence, cybersecurity, and covert social media operations.

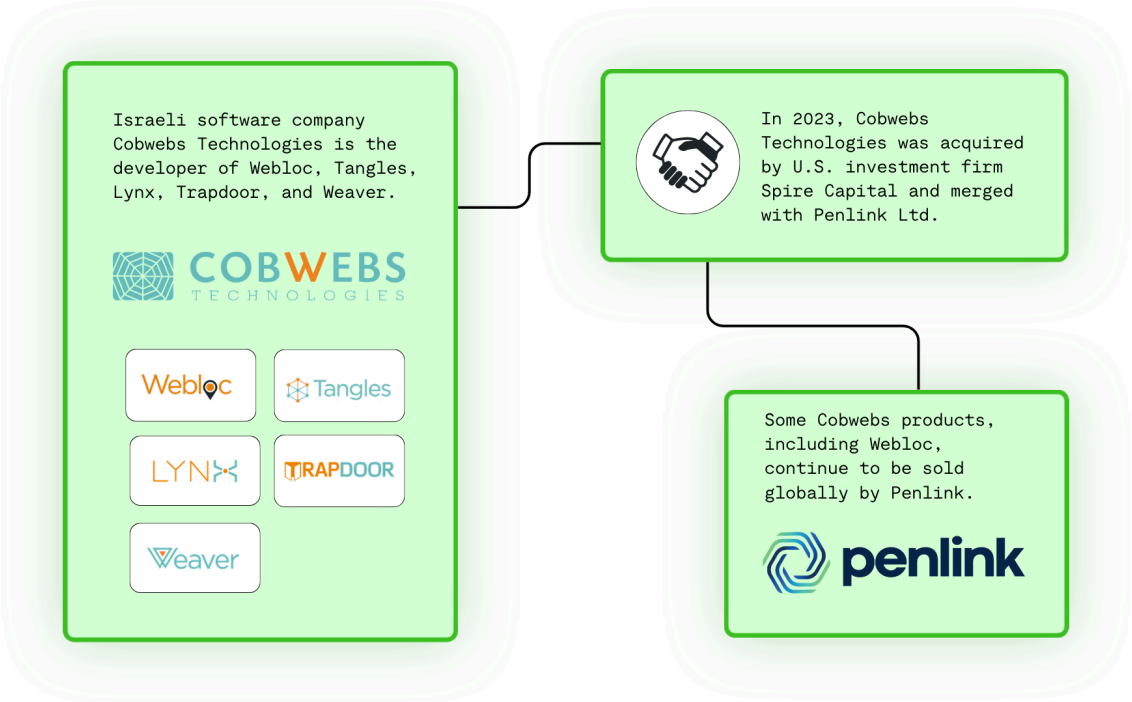


Figure 1: Webloc and other products developed by Cobwebs Technologies are now sold by Penlink.

[4] Cobwebs Technologies Ltd (Israel), Cobwebs Technologies UK Ltd (UK), Cobwebs America Inc (U.S.), Cobwebs GmbH (Germany), Cobwebs Asia Pte Ltd (Singapore), Cobwebs Pacific Ltd (New Zealand)

[5] Cobwebs Technologies Ltd based in Israel became Penlink Technologies Ltd, Cobwebs Technologies UK Ltd became Pen-link Technologies UK Ltd, Cobwebs GmbH based in Germany became Pen-link GmbH

Cobwebs' Core Product: Tangles

Developed by Cobwebs Technologies, Tangles is a software platform that provides access to data from social media and the open, deep, and dark web. It has been referred to as a "web investigation platform," "web intelligence platform" or "WEBINT" system. According to leaked training manuals, government and commercial customers can search for keywords and personal identifiers like names, email addresses, phone numbers, and usernames to identify online accounts and then analyze what they post, their interactions, relationships, activities, event attendances, and interests. They can monitor and profile individuals, create "target cards," receive alerts, analyze geolocation information extracted from posts and photos, and perform network analyses, for example, to identify groups based on their mutual friends or workplaces.

According to service definitions in U.S. procurement records,[6] data sources include web forums, blogs, text storage sites (also known as pastebins) and social media platforms such as Facebook, Instagram, Twitter/X, YouTube, LinkedIn, SnapChat, TikTok, Reddit, VK, Weibo, Parler, and Gab. They also include the dating platform Tinder and "messaging sources" such as Telegram, Viber, and Truecaller. Tangles also analyzes information from Facebook and Telegram groups, Facebook Marketplace, and the payment service Venmo.

The system's image processing module detects objects and landmarks in a given photo. It also provides facial recognition, and includes the capability to search for individuals based on their photos, according to a leaked technical proposal related to a contract in El Salvador. Tangles focuses on publicly available data and is now promoted by Penlink as an "open source intelligence" platform powered by "AI." It is not clear whether Tangles incorporates personal data purchased from data brokers.

Other Products Developed by Cobwebs

Webloc

The ad-based surveillance system Webloc, which is the main subject of this report and further examined in the next sections, analyzes data on the behaviours and movements of hundreds of millions of people. In contrast to Tangles' focus on publicly available data from the web and social media, Webloc relies on data purchased from mobile apps and digital advertising. It relies on the re-purposing of behavioural data originally collected for the purposes of operating consumer apps or delivering ads for surveillance. The lawfulness of such repurposing is addressed in **Section 10**. Introduced in 2020, Webloc provides the capability to covertly monitor the whereabouts, movements and personal characteristics of entire

[6] "Scope of work" specifications in the 2023 Tangles contract of the police department of the City of Elk Grove, California: https://www.eff.org/files/2025/08/18/cpra_-_elk_grove_pen-link.pdf, "Scope of Services" specifications in the 2023 Tangles contract of the police department of Panama City Beach, Florida: https://www.pcbfl.gov/home/showpublisheddocument/23158/638271635414570000, accessed 10.3.2026

populations. It is sold as a Tangles add-on product, but customers have to purchase a separate Webloc license in order to use it, according to our research about Webloc customers in the U.S.

Lynx

Lynx is another Tangles add-on product that provides investigators and intelligence analysts with the capability to anonymously browse the web and use social media platforms with fake identities and accounts via what is advertised as a global proxy infrastructure. In 2020 and 2021, Cobwebs Technologies promoted Lynx as a system for "Virtual HUMINT Operations" that helps create, manage, and maintain "virtual agents" with the "click of just one button." According to a leaked technical proposal related to a contract in El Salvador, Lynx provides "avatar management" and "virtual agents" across "email, social networks, forums" with "support for various social media platforms."[7] Documents obtained from the Los Angeles Police Department (LAPD) via a freedom of information request describe Lynx as a system to "collect data from various virtual HUMINT sources online" by "creating and using avatars (virtual agents)." Media reports and public records suggest that Lynx was purchased in El Salvador and by U.S. federal agencies like DHS and the Internal Revenue Service (IRS). We do not know whether Lynx is still being sold by Penlink.

Trapdoor

Another product named Trapdoor has been rarely reported or mentioned anywhere. In 2021, Cobwebs Technologies promoted Trapdoor on its website as a system for "active web intelligence." As briefly examined in **Section 8**, a specifications document and technical analysis suggest that Trapdoor is a "social engineering platform" that helps customers to create fake web pages and send phishing links to victims in order to trick them into revealing information, including passwords. Our own analysis further suggests that Trapdoor allows customers to extract device information such as battery level, access a device's camera and microphone, remotely open hidden tabs in the victim's web browser and deliver "payloads" to them. Based on our analysis, we assess that Trapdoor can help facilitate the deployment of malware on a victim's device but does not include remote device infection or malware capabilities itself. We do not know whether Trapdoor is still being sold by Penlink, and we could not identify any Trapdoor customers. During our analysis of Cobwebs Technologies' server infrastructure, we identified active servers located in Kenya and Indonesia that display Trapdoor login pages in the web browser and four additional servers that may be associated with Trapdoor deployments.

Weaver

Weaver was promoted as a "financial investigation platform" that helps financial institutions address everything from fraud, money laundering, and cyber threats to reputation risks through monitoring "natural persons, companies, and other entities seeking to become clients, partners, or employees of the institution." We assume that Weaver is basically a Tangles version for financial institutions. We could

[7] Translation by the authors, original in Spanish: "manejo de avatares," "fácil manejo de agentes virtuales en diversas plataformas: correos, redes sociales, foros, etc," "avatars management ... Apoyar diferentes plataformas de medios sociales"

not identify any Weaver customers. During our analysis of Cobwebs Technologies' server infrastructure, we identified one active server displaying a Weaver login page in the browser.

Threat Intelligence Platform

Cobwebs Technologies also provided a **Threat Intelligence Platform** that relies on "huge sums of data" from the "open, deep, dark web and external sources." We assume that this product is or was a Tangles version for the cybersecurity sector. We could not identify any customers.

Penlink

Since 2023, Tangles and Webloc have been sold by Cobwebs successor Penlink, according to our research on Webloc customers. We do not know whether Lynx, Trapdoor, Weaver, and other products developed by Cobwebs Technologies are now also being sold by Penlink. They are not promoted on Penlink's website. However, we identified servers active in 2026 that show login pages for Weaver and Trapdoor in the browser, according to technical analysis. In its response to the Citizen Lab, Penlink claims, without being specific, that our report describes "products that no longer exist."

Penlink is a surveillance technology vendor based in the U.S. Founded in 1987, it provides software that helps law enforcement agencies wiretap telecommunications customers and social media users based on warrants. Penlink's PLX product helps to retrieve, organize, and analyze call records, search histories, login data, and other information from AT&T, Verizon, T-Mobile, Comcast, Google, Facebook and other companies. In 2022, Penlink had contracts worth $20 million a year with U.S. federal agencies like ICE, FBI and DEA and many other contracts with local and state police, according to Forbes.

According to its website, Penlink is now selling PLX, Tangles and other products including CoAnalyst, a "digital investigation" platform utilizing "generative AI." A promotional document published by journalist Joseph Cox in 2026 describes Penlink's "digital intelligence package for national security" consisting of Tangles, Webloc and another product not mentioned anywhere else, WebEye. Originally in Portuguese, the document describes WebEye as a system for "investigations of web pages and browser session extraction." In Penlink's response to this report, the company describes itself as "committed to delivering tools for law enforcement to rapidly search, analyze, and identify threats to keep our communities safe" and claims that its "customers use these tools and capabilities to locate kidnapped children, combat human and drug trafficking, and identify potential terror threats, among other critical uses."

Concerns and Public Controversy

The use of Webloc to collect data from mobile apps and digital advertising from entire populations for covert surveillance, which is further examined in the next sections of this report, raises massive concerns about civil liberties, warrantless surveillance, and data protection, as discussed in **Section 10**.

However, it is not only Webloc that generated controversial public debate in recent years:

- **Meta** mentioned Cobwebs Technologies prominently in its 2021 "Threat Report on the Surveillance-for-Hire Industry," banning it from its platform and explaining that "accounts used by Cobwebs customers also engaged in social engineering to join closed communities and forums and trick people into revealing personal information." Meta "identified customers in Bangladesh, Hong Kong, the United States, New Zealand, Mexico, Saudi Arabia, Poland" and "observed frequent targeting of activists, opposition politicians and government officials in Hong Kong and Mexico." Cobwebs Technologies stated that the report was "false," because "We do not provide avatars" and Meta had mentioned "countries that are not related to us."
- In 2020 and 2021, Cobwebs Technologies presented sessions titled "Tactical Web Intelligence (WEBINT) & Social Engineering: Gathering Actionable Intelligence via a powerful WEBINT platform" at ISS World, a trade event which markets surveillance technologies for government intelligence, law enforcement and military agencies.
- The DHS used Tangles to compile dossiers on Black Lives Matter protesters in Portland in 2020, according to an internal DHS report published by U.S. senator Ron Wyden, leading to concerns over the creation of those dossiers being politically motivated.
- In a leaked 2020 training manual, Cobwebs Technologies prominently showed profiles of Black Lives Matter **activist groups, protesters, and a journalist** as examples of targets to be monitored via Tangles. Two years later, as political power in the U.S. had changed, another leaked Tangles manual explained how to target January 6th protesters. Also in 2020, the company offered a webinar titled "Radical Civil Unrest" discussing "how radical civil unrest is woven thru the fabric of the deep web" and covering topics such as "[d]oxing, a threat to government symbols and structures, organized and potentially violent networks discovery" [sic]," according to documents from the LAPD obtained via a freedom of information request.
- The intelligence unit of **Immigration New Zealand**, an agency responsible for border control, issuing visas and managing immigration, used Tangles from 2019 to 2024 to scan people's social media accounts, according to several media articles. It was used on a "known human smuggler," an "irregular migration actor" and other targets, according to an internal audit. The immigration minister stated that it was used to protect the country from people "who might pose a risk" given that the agency was processing 600,000 visas a year. In 2024, an "automated register of false personas to use on social media platforms" was set up, according to documents obtained via a freedom of information request. This suggests that the New Zealand government might have purchased not only Tangles, but also Lynx.
- In 2023, Cobwebs Technologies announced that it will provide its Tangles system to a private intelligence outfit in the U.S. run by **religious fundamentalists**, who claim to "hunt" pedophiles and track sex workers in the name of the fight against sex trafficking, according to the *Intercept*. A Cobwebs Technologies employee wrote in a blog post that he was "proud" to "represent" the company and "volunteer" his time to this "worthwhile organization." This suggests that Cobwebs Technologies provided its capabilities to a private, politically motivated actor, exposing private information of vulnerable groups.

The findings laid out in the next sections raise additional concerns, from the intrusive nature of Webloc, its customers and potential uses to the links between Cobwebs Technologies and the spyware industry.

3. Webloc

Cobwebs Technologies announced the introduction of Webloc in 2020 and promoted it as a "location intelligence platform" that is "designed to meticulously race through and scan endless digital channels from the web ecosystem, collecting and analyzing huge sums of location-based data." According to its 2021 website, Webloc "provides access to vast amounts of location-based data in any specified geographic location," relying on "billions of data points" from "different types of large datasets." Soon thereafter, Cobwebs removed the page on Webloc from its website.

While the web intelligence system Tangles has always been heavily promoted, information on Webloc has notably disappeared from public view in recent years. As of 2026, Webloc is mentioned only once on the Penlink website. On a page about a Tangles training course, Penlink offers a "Webloc Fundamentals" course.

Cobwebs Technologies and its successor Penlink do not provide much robust information about Webloc's capabilities and data processing practices. Our analysis in this section is largely based on documents dated 2021, 2022 and 2023, including a leaked technical proposal, technical specifications we discovered on the web, Webloc release notes we received from a research partner and public records related to Webloc contracts. A Penlink document that we believe was created in 2025 confirms the basic capabilities identified in our analysis but provides less detail. Further, in response to this report, Penlink provided some additional information regarding Webloc.

Location Surveillance with Webloc

We obtained from a research partner a leaked document related to a Webloc contract with El Salvador National Civil Police. This document provides a comprehensive overview of Webloc including several screenshots of the user interface. The document, dated February 2021, is titled "Technical Proposal" (Spanish original "Propuesta Técnica"), and comes from the Mexican company EyeTech Solutions, who resold Tangles, Lynx and Webloc to El Salvador police, as reported by *El Faro* in 2023. We have reproduced the leaked document here.[8]

According to the document, Webloc provides access to a constantly updated stream of geolocation records from 500 million phones and other mobile devices from across the globe.

[8] The document, dated February 2021 and titled "Technical Proposal," sets out what the Mexican Cobwebs reseller Eyetech Solutions offered to El Salvador National Civil Police. It contains descriptions of Tangles, Webloc and Lynx. The product descriptions have significant overlaps with descriptions from other sources reviewed in the report. The user interface shown in the example screens is almost identical to the user interface shown in other sources reviewed in the report. According to our analysis, we have high confidence in the authenticity of the document.

The screenshot in **Figure 2** (below) shows the Webloc user interface. In this example, the system tracked a male person currently located in Abu Dhabi, who has 141 apps installed on his mobile phone, some of which sent 81 different GPS location coordinates to the system over the past five days. In addition, he was apparently located based on Wi-Fi access points nearby his phone 110 times. The activity graph on the right bottom indicates that the system tracked his location up to 12 times a day.

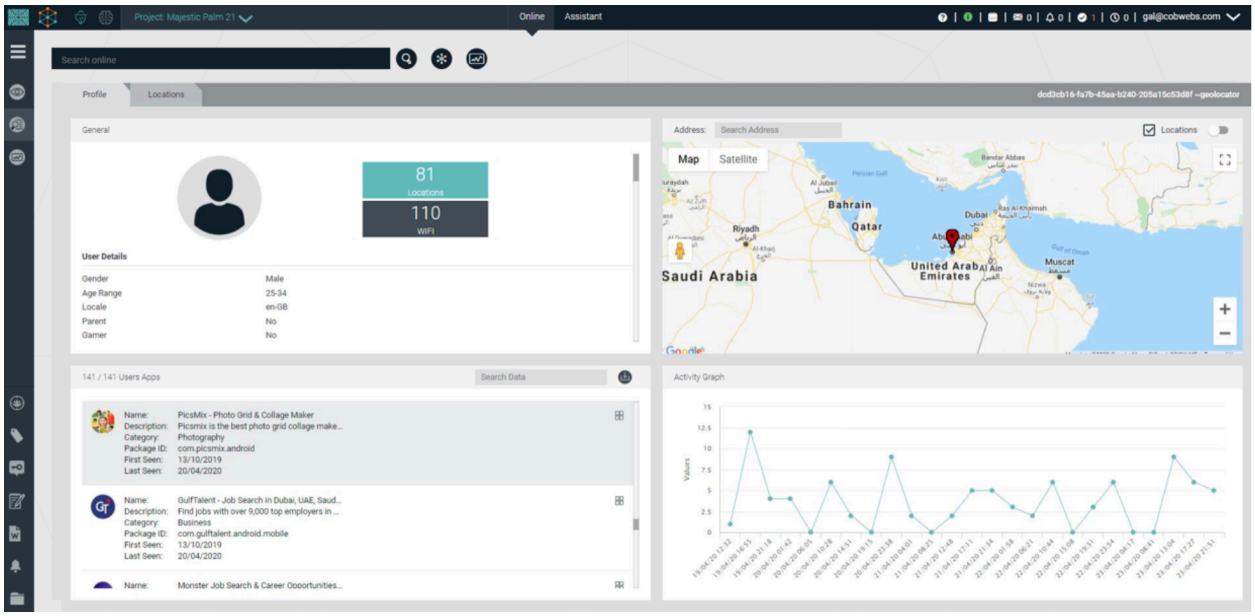


Figure 2: Webloc example screen taken from the El Salvador document

The person's profile and location records are linked to a unique identifier, displayed in the screen at the right top above the map. This type of identifier is known as a mobile advertising ID and represents a unique identifier assigned to his phone.

Another example screen demonstrates how Webloc tracked a person travelling from Germany via Austria to Hungary, based on analyzing 39 past location records out of 500 recorded by the system.

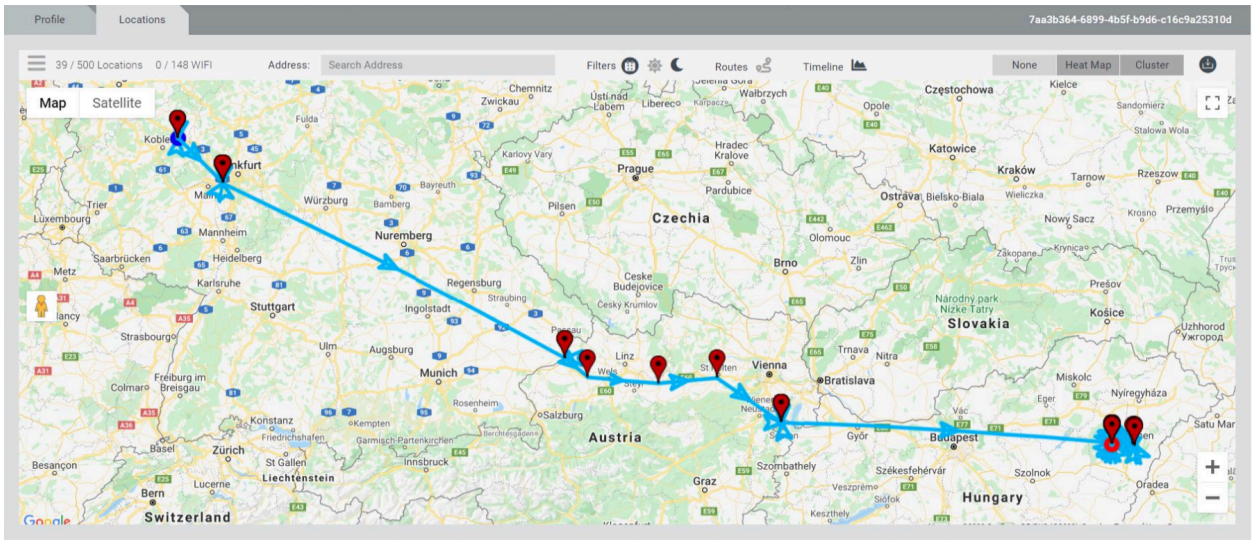


Figure 3: Webloc example screen taken from the El Salvador document.

Webloc customers can start a surveillance operation by searching for mobile devices that were present in a certain area, which is referred to as a “perimeter” or “geofence." They can also identify devices that were located in two or more defined areas within a certain period of time, indicating persons travelling from one place to another, according to the El Salvador document.

The screenshot in **Figure 4** shows Webloc displaying a list of 1,433 location records of persons whose mobile devices were located in certain areas in both Italy and Romania within a certain time period. For two devices, identified by their mobile advertising IDs, the system captured three location records in both Italy and Romania.

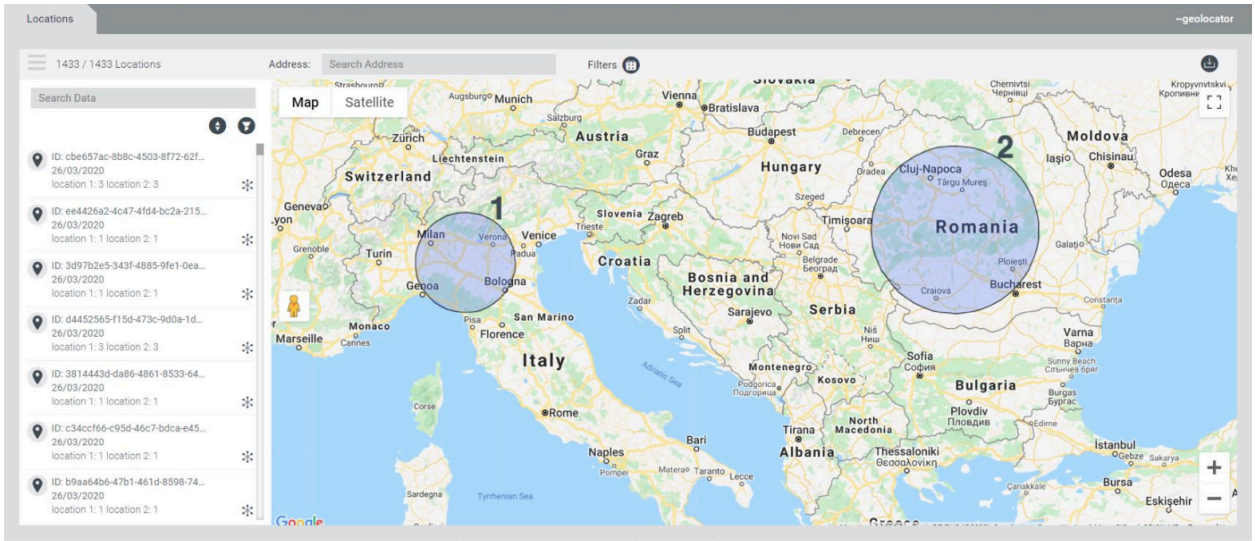


Figure 4: Webloc example screen taken from the El Salvador document.

Another example screen (**Figure 5**) from the El Salvador document illustrates how Webloc visualizes the driving or walking routes of persons located within a few blocks in a Tel Aviv neighborhood, and includes a timeline. In total, the system tracked the locations of 103 persons in the area.

Figure 5: Webloc example screen taken from the El Salvador document.

Webloc is not limited to location tracking; it provides access to a wide range of information about each person whose phones are constantly broadcasting personal data to digital advertising firms or data brokers via the apps installed on their devices.

The table in **Figure 6** (below) from the El Salvador document presents an example user profile for a male person aged 18-24 located in Hungary who uses a Samsung Galaxy S8 Android phone with the device language set to English. In addition, it lists a set of “user segments” that describe characteristics and behaviours typically used for ad targeting in digital marketing. In this example, the person was classified as a regular commuter who is interested in basketball and buying luxury goods. The profile also indicates whether the tracked person is a parent, a gamer, or a traveller.

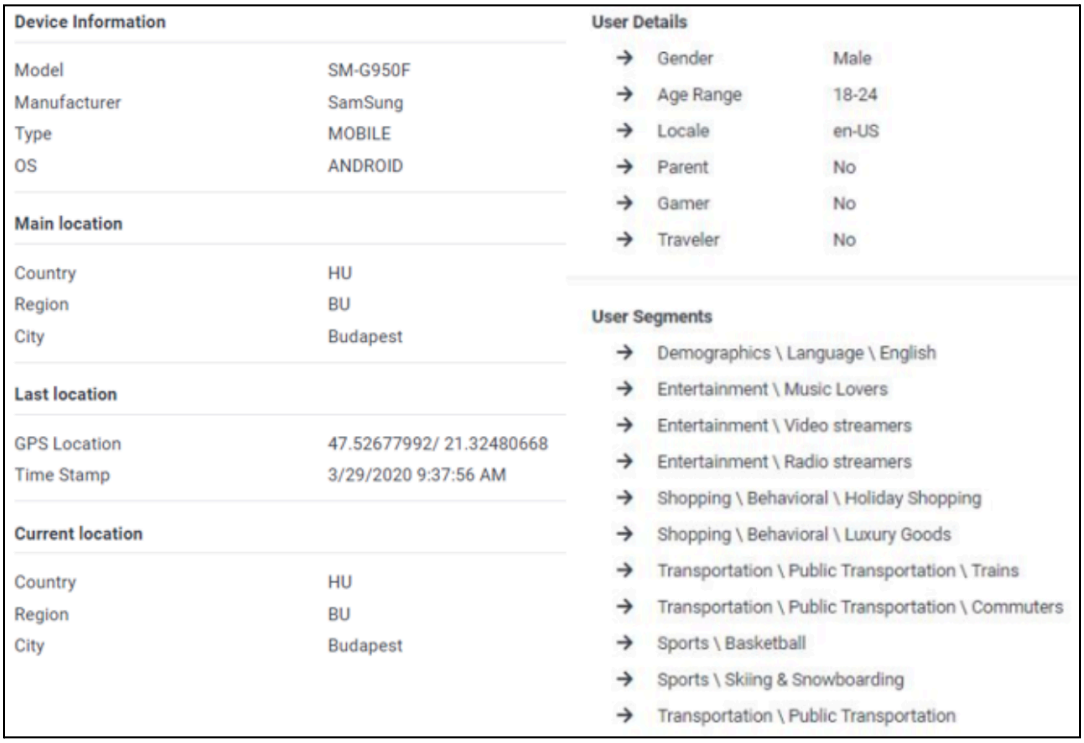


Figure 6: Webloc table on profile attributes taken from the El Salvador document.

The “user segments” section in the profile shows ad targeting categories typically used in digital advertising, which specifically suggests that Webloc obtains data from sources that are related to digital advertising. While the attributes shown in the example screen relate to personal characteristics that may seem not too sensitive, many segment attributes typically used in digital advertising reveal everything from employment, political views, religion and sexual orientation to pregnancy, health issues or personal debt.

Additional Webloc Sources

We analyzed additional documents that contribute to our understanding of Webloc. A document[9] related to a contract that was published in 2021 by the Office of Naval Intelligence, the U.S. Navy’s military intelligence agency, indicates that Webloc provides the ability to "continuously monitor unique mobile advertising IDs” for both Android and iOS devices,[10] linked to geolocation data including Wi-Fi location, device information, age, gender, language, interest categories, and data on the apps “installed and used."

[9] https://govtribe.com/file/government-file/lsj-rfq-ssa-geoint-webloc-swa-dot-pdf, accessed on 13.3.2026
[10] Notably, the Navy document specifically mentions “IDFA and IDFV support” in relation to Apple’s tracking transparency system ATT.

According to a Vietnamese “Technical specifications” document dated 2021 and branded “Cobwebs Technologies," Webloc collects and analyzes mobile records that contain advertising ID, timestamp, geolocation coordinates based on GPS or Wi-Fi, IP address, carrier information, Wi-Fi name, device type and operating system, age, gender, locale, apps used and ad targeting segments.[11] It emphasizes the same three profile categories (parent, traveler, gamer) as mentioned in the El Salvador document and suggests that Webloc provides functionality to export the raw data in CSV format.[12]

A Penlink-branded promotional document[13] published by the journalist Joseph Cox in 2026 confirms that Webloc provides very similar capabilities today. The document was created in 2025, according to PDF metadata. It is written in Portuguese and describes a “digital intelligence package for national security” consisting of Tangles, Webloc and other products. An example screenshot shows location records associated with advertising IDs and a list of apps installed on a phone. Another document discussed by Cox suggests that Webloc has added the capability of inferring location from IP addresses, supplementing the systems’s GPS and Wi-Fi location capabilities.

Identifying People via Webloc

As discussed in the background section, advertising IDs referring to mobile devices can be used to track, follow, profile, and identify the persons who use those devices. Many parties can easily retrieve the name, email address and phone number associated with an advertising ID, and vice versa. Even if it was not possible to link the pseudonymous device identifier utilized by Webloc to a name, location records can still identify individuals in many ways.

Identifying the persons behind the devices is the declared purpose of Webloc. The El Salvador document emphasizes that it would be vital for analysts who use Webloc to identify the actual person behind the device, for example by identifying their home addresses and workplaces.

[11] Accessed on 12.3.2026 and archived by the authors: https://www.studocu.vn/vn/document/hoc-vien-cong-nghe-buu-chinh-vien-thong/ki-thuat-lap-trinh/7-webint-specifications/118733920,

[12] Translated from Vietnamese by the authors: “The Web-Location platform will allow exporting the refined data to CSV format containing Advertising ID, Timestamp, Local Timestamp, Source, Address, Latitude, Longitude, Accuracy, IP Address, Connection Type, Location Name, Carrier Information if available.”

[13] https://www.scribd.com/document/894221538/DoD-Pager-Portuguese, accessed 20.3.2026

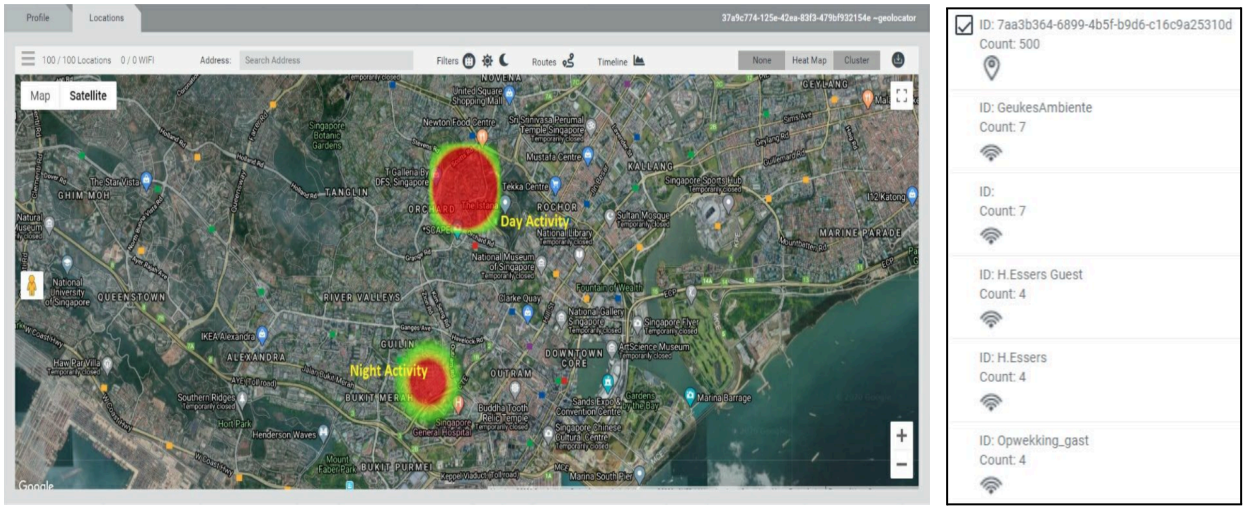


Figure 7: Webloc example screen taken from the El Salvador document.

The system's heat map functionality can show where a device was typically located during the day and night. Referring to the example screen in **Figure 7** (on the left) displaying a map of Singapore, the document explains that it would be safe to deduce the home address and workplace based on the map shown in this example (see **Figure 8**). The document also suggests sending "ground forces" to locations associated with a "suspect."[14] As detailed in **Section 5**, local police in Tucson, Arizona, explained in an internal report how it used Webloc to identify the apartment address and workplace of a person and his romantic partner.

Determinación de mapas de calor basados en la actividad para rangos diurnos - El mayor tiempo que pasa el sospechoso en un lugar durante diferentes momentos del día también es información valiosa. WebLoc permite a los usuarios filtrar rápidamente los patrones de actividad del dispositivo en función del tiempo pasado en diferentes ubicaciones en forma de mapas de calor. Esta informacion está en relación con el tiempo pasado en un lugar. La cantidad de señales recibidas para una ubicación será directamente proporcional al tiempo pasado allí y conducirá a un mapa de calor más grande. En la siguiente figura, podemos ver claramente la actividad diaria de un dispositivo en dos ubicaciones diferentes. Sería seguro deducir del mapa a continuación que estas ubicaciones se pueden asumir de manera segura como lugar de trabajo (actividad diurna) y residencia (actividad nocturna) para la persona que posee el dispositivo.

Figure 8: Excerpt from the El Salvador document on determining a person's home address and workplace.

[14] Translated by the authors, original in Spanish: "sospechoso," "fuerza terrestre"

Both the El Salvador and the Vietnam documents explain that the names of Wi-Fi access points[15] a tracked individual connected to, as shown in **Figure 7** (right), can reveal last names, workplaces or other venues visited by them.

According to a document related to a Webloc contract with a U.S. law enforcement agency,[16] the system provides “special agents” with an “unapparelled [sic] ability to develop investigative leads." The U.S. Navy document states that Webloc provides the capability to “find and establish relevant and meaningful relationships and connections to individual's virtual and physical patterns of life." To “enhance target identification and tracking," the system could additionally combine mobile advertising data with imported “cellular data dumps," likely referring to phone and geolocation data obtained from telecommunications network operators.

Webloc can display location records not only on a map but also in Google Street View, as the example screen (**Figure 9**) from the El Salvador document illustrates. It shows multiple records represented by red pins, all of them possibly associated with the same person who was frequently located in front of a certain house in St. Petersburg, Russia.

Figure 9: Webloc example screen taken from the El Salvador document.

[15] According to the Vietnam document, Webloc records both BSSID and SSID.

[16] “Statement of Work” dated March 2023 related to a contract with the Office of Justice Services (OJS), Bureau of Indian Affairs (BIA), Department of the Interior (DOI); FOI document via Jack Poulson, from p. 21: https://techinquiry.org/FOIA/Cobwebs-BIA.pdf, accessed 22.7.2025; archived: https://web.archive.org/web/20230730233450/https://techinquiry.org/FOIA/Cobwebs-BIA.pdf

Mobile Location Dragnet

Webloc supports a variety of query and network analysis capabilities, ranging from queries for location records linked to a particular known mobile device ID to retrieving records for all devices that were observed in one or several specified areas, according to the El Salvador and Vietnam documents. The system can send alerts when monitored devices are located at a new place or when new devices enter a monitored area.

A document titled “Webloc Release Notes 6.5” we received from a research partner dated September 2022, explains how the system’s “Cross Analysis - Connections” tool can help reveal associations between devices and their owners based on the places they have visited, as illustrated in the example screen in **Figure 10**.

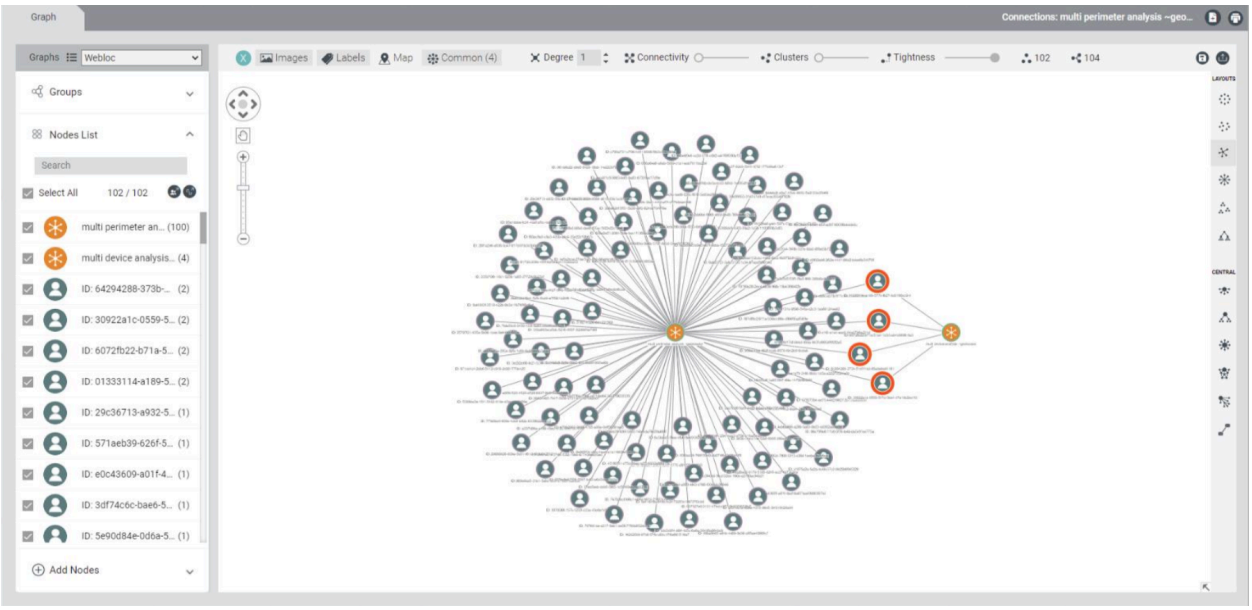


Figure 10: Webloc example screen taken from the “Webloc Release Notes” document.

Historical Data and Update Frequency

Webloc provides both historical data and a constantly updated stream of new location records. According to the El Salvador and Vietnam documents, the data is updated every four to 24 hours. The system provides three years of historical data, according to a 2023 document related to a Webloc contract with a U.S. law enforcement agency.

Types of Personal Data Processed

The following table summarizes the types of personal data processed by Webloc as of 2021, according to the El Salvador, Vietnam, and U.S. Navy documents:

Data category	Description
Personal identifiers	Mobile advertising ID for Android and iOS devices, IP address
Timestamp	Each record has a timestamp
Geolocation	GPS coordinates, Wi-Fi location, precision
Inferred geolocation data	Home location, work location, most visited locations
Wi-Fi data	SSID, BSSID, connection status
Device information	Device model, manufacturer, type, operating system
Personal characteristics	Age, gender, locale/language, parent (y/n), traveller (y/n), gamer (y/n)
Behavioural profile	Segments / ad targeting categories, e.g. “Demographics / Language / English," “Transportation / Public Transportation / Commuters," “Shopping / Behavioral / Luxury Goods”
Apps used	List of mobile apps used, including the period of time each app was seen on the device

Table 1: Data categories processed by Webloc

The documents claim that data collection complies with the General Data Protection Regulation (GDPR) and “various” privacy laws and that it is collected with the “consent” of those who are monitored by the system. We further discuss those claims in **Section 10**.

In its response to the Citizen Lab, Penlink says that Webloc “contains only location data (sometimes precise, and sometimes non-precise location data) tied to device identifiers. It does not include age, gender, parenthood, interest categories, or website visited.” We cannot verify this claim. Even if age, gender and interest categories were not included in Webloc anymore, location records reveal information about someone’s habits, interests and personal characteristics. A Penlink-branded document[17] published by the journalist Joseph Cox, which was created 2025 according to PDF

[17] https://www.scribd.com/document/894221538/DoD-Pager-Portuguese, accessed 20.3.2026

metadata, explains that Webloc "generates demographic insights" and facilitates "detailed identity and lifestyle pattern resolution".[18]

We generally consider data that is linked to Advertising IDs as related to digital advertising. While Penlink's response to the Citizen Lab and privacy policy refer to "device identifiers", the company's Privacy Choices page specifically mentions the "Advertising ID."

Data Sources, Coverage, and Quality?

Public reporting provides information on how similar ad-based surveillance vendors in the U.S. obtain the data, which data brokers they bought from, and how they participated in the digital advertising sector themselves. Yet, despite spending a considerable amount of resources investigating potential Webloc data supply chains, it remains opaque to us. We are currently not able to make a solid conclusion about how PenLink obtains Webloc data today. It might obtain data from SDK-based sources, RTB-based sources or a mix of both, either directly or indirectly via other data brokers.

Several sources, including the El Salvador and Vietnam documents, both dated 2021, suggest that Webloc obtains data via third-party tracking software embedded in mobile apps, often referred to as mobile app SDKs. The documents show how Webloc displays data on Wi-Fi access points, including their names. SDK-based data sources can potentially access Wi-Fi data. Sources that obtain the data from the RTB bidstream in digital advertising cannot access it. This suggests that Webloc actually obtained the data from SDK-based sources in 2021.

However, several attributes processed by Webloc in 2021 are often obtained from RTB-based sources, including age, gender, and the attributes related to user segments and ad targeting categories. These attributes may be also accessible via mobile app SDK. Whether obtained from SDK-based or RTB-based sources, these attributes clearly indicate that the data is associated with digital advertising.

Almost certainly, Webloc's data sources are different in 2026. The data supply chains for surveillance technology vendors that obtain data from mobile apps and digital advertising are constantly changing. Data brokers that harvest data on behalf of ad-based surveillance vendors have been repeatedly cut off from their app data sources.

According to the El Salvador document, Webloc obtained data from 500 million mobile devices that were tracked at least once in a month in 2021, with global coverage that varies per region. We are not able to assess the actual current coverage, quality, and accuracy of the data processed by Webloc.

[18] We generally consider data that is linked to Advertising IDs as related to digital advertising. While Penlink's response to the Citizen Lab and privacy policy refer to "device identifiers", the company's Privacy Choices page specifically mentions the "Advertising ID".

4. Webloc Customers

This section analyzes and documents what we know about the customers and uses of the geolocation surveillance system Webloc.

First, we present a summary of U.S. customers including federal agencies such as ICE, the U.S. military and law enforcement agencies in several states, cities, and counties, based on a systematic screening of media reports, public records and responses to freedom of information requests. In addition to widely reported customers, we identified a number of contracts that were rarely or not yet reported to our knowledge.

Secondly, alongside reporting from Szabolcs Panyi at *VSquare*, we show that domestic intelligence in Hungary uses Webloc. These are novel findings that have not been previously reported.

Thirdly, we document El Salvador National Civil Police's purchase of Webloc in 2021 and 2022, which was rarely reported outside the country.

U.S. Federal Agencies

Immigration and Customs Enforcement (ICE)

Current Webloc customers include Immigration and Customs Enforcement (ICE), the controversial federal agency that was involved in fatal shootings that may amount to extrajudicial killings and has been accused of routine detainments without warrants and probable cause. ICE purchased Tangles and Webloc licenses worth up to $2.3 million for the term of September 2025 to September 2026, according to a publicly available document[19] related to the contract[20] first reported by *404 Media*.

The Office of Intelligence of Homeland Security Investigations (HSI), one of the two ICE law enforcement units, uses the system to "support domestic and international investigations into cross-border crimes," according to the document. ICE had already bought licenses for Cobwebs and Tangles between 2022 and 2025.[21] A pricing proposal obtained by Tech Inquiry via a freedom of information request suggests that the 2022-2023 contract also included Webloc.

[19] https://sam.gov/workspace/contract/opp/b92458a603f24cb5926eafe26829cde5/view, accessed 16.3.2026

[20] https://www.usaspending.gov/award/CONT_AWD_70CMSD25P00000138_7012_-NONE-_-NONE-, accessed 16.3.2026

[21] https://www.usaspending.gov/award/CONT_AWD_70CMSD23P00000145_7012_-NONE-_-NONE-, https://www.usaspending.gov/award/CONT_AWD_70CMSD22P00000108_7012_-NONE-_-NONE-, accessed 16.3.2026

In 2023, the Department of Homeland Security (DHS) released an internal report[22] which found that several DHS entities, including ICE, violated federal law through their purchases of "commercial telemetry data (CTD) collected from mobile devices that included, among other things, historical device location." The report does not mention vendors but confirms that ICE had been purchasing such data starting in 2019. ICE stated that it had stopped using the data in late 2023. We consider ICE a confirmed Webloc customer in 2025-2026 and a potential Webloc customer in 2022-2023.

U.S. Military

The U.S. military purchased Webloc on at least two occasions. In 2021, the Navy's military intelligence agency, the Office of Naval Intelligence, purchased annual Webloc licenses, according to a publicly available document related to the contract,[23] first reported by one of the authors of this report.[24] In 2022, The U.S. Army Space and Missile Defense Command (USASMDC) purchased annual Tangles and Webloc licenses[25] as part of a large contract awarded to the defense contractor Science Applications International Corporation (SAIC),[26] which was not reported to our knowledge. We consider the U.S. Navy's Office of Naval Intelligence a confirmed Webloc customer in 2021-2022 and the U.S. Army's USASMDC a confirmed Webloc customer in 2022-2023.

Customer	Contracts
Immigration and Customs Enforcement (ICE), Department of Homeland Security (DHS)	Sep 2025 - Sep 2026, Tangles and Webloc licenses worth up to $2.3M 2023 - 2025, Cobwebs/Tangles licenses worth $3.4M 2022 - 2023, Cobwebs Tangles licenses worth $225,060, very likely including Webloc according to a pricing proposal
United States Army Space and Missile Defense Command (USASMDC), U.S. Army	2022 - 2023, Tangles and Webloc
Office of Naval Intelligence, U.S. Navy	2021 - 2022, Webloc
Bureau of Indian Affairs Police (BIA-OJS), Department of the Interior	2023 - 2025, Tangles and Webloc

[22] https://www.oig.dhs.gov/sites/default/files/assets/2023-09/OIG-23-61-Sep23-Redacted.pdf, accessed 16.3.2026

[23] https://govtribe.com/file/government-file/lsj-rfq-ssa-geoint-webloc-swa-dot-pdf, accessed 28.3.2022

[24] https://x.com/WolfieChristl/status/1508553279181135873, accessed 16.3.2026

[25] https://www.usaspending.gov/award/CONT_AWD_W9126020FD504_9700_W9113M17D0007_9700, accessed 16.3.2026

[26] https://www.usaspending.gov/award/CONT_IDV_W9113M17D0007_9700, accessed 16.3.2026

Table 2: Purchase of Webloc and other Cobwebs products by U.S. federal agencies

Bureau of Indian Affairs Police

Documents suggest that the Bureau of Indian Affairs Police (BIA-OJS), a law enforcement unit of the U.S. Department of the Interior's Bureau of Indian Affairs (BIA), purchased Webloc. In 2023, BIA entered a five-year Tangles contract on behalf of BIA Police, according to contractual documents obtained by Tech Inquiry via a freedom of information request. While the contract does not mention Webloc, it clearly describes Webloc capabilities.

The contract's "statement of work" requires a system that provides the ability to "view geo-signals such as those provided by mobile applications which have location data associated with it," "track phones/mobile devices through their Mobile Advertisement ID (MAID)" and "track the mobile device's location history." According to public records,[27] the contract's renewal option was exercised only once in 2024, which suggests that the contract ended in 2025. We consider BIA Police a Webloc customer from 2023 to 2025.

U.S. State and Local Customers

Department of Homeland Security of West Virginia

The Department of Homeland Security (DHS) of West Virginia has been a Webloc customer since 2021. DHS West Virginia Fusion Center entered two three-year contracts including both Tangles and Webloc, one beginning in 2021, and the other in 2024. The effective end date of the 2024 contract (which consists of an initial one-year period and two subsequent one-year periods that are subject to annual renewals) is June 2027. We are not aware of public records confirming annual renewals. We consider DHS West Virginia a confirmed Webloc customer from 2021 to 2025 and a potential Webloc customer until 2027.

Texas Department of Public Safety

The Texas Department of Public Safety (DPS) is also a long-term Cobwebs customer. As first reported by the *Intercept*, Texas DPS initially purchased Tangles and Webloc in 2021 as part of the Texas Governor's "Border Disaster" efforts. The initial annual contract on behalf of the Texas DPS' Intelligence and Counterterrorism division worth $198,000 included both Webloc and Lynx, according to media reporting and documents obtained via freedom of information requests shared with the Citizen Lab.

Texas DPS also purchased Tangles in 2022 and 2023. In 2024, it entered into a five-year Tangles contract worth $5.3 million for 230 users, according to the *Texas Observer*. In response to records

[27] https://www.usaspending.gov/award/CONT_AWD_140A1623C0002_1450_-NONE-_-NONE-, accessed 16.3.2026

requests for the years 2023 and 2024, Texas DPS stated to have seven investigative reports and no incident reports that mention the terms “Cobwebs” or “Tangles." It refused to release the documents for public safety reasons. We consider Texas DPS a confirmed Webloc customer from 2021 to 2022 and a potential Webloc customer from 2023 to 2029.

Customer	Contracts
DHS West Virginia, Fusion Center	Jul 2024 - Jun 2027, Tangles and Webloc, three-year contract subject to annual renewals 2021 - 2024, Tangles and Webloc
Texas Department of Public Safety (DPS)	2021 - 2022, Tangles and Webloc 2021-2024 and 2024-2029, Tangles, the latter representing a five-year contract worth $5.3M
Los Angeles Police Department (LAPD), California	2022 - 2023, Tangles and Webloc
Dallas Police Department (DPD), Texas	2025, Tangles and Webloc 2025 - 2028, Tangles, likely including Webloc for the entire three-year contract
Baltimore County Police Department, Maryland	2024 - 2027, Tangles and Webloc, three-year contract subject to annual renewals 2022 - 2023, Webloc 2020 - 2022, Tangles; 2023-2024 Cobwebs supplier contract
Tucson Police Department (TPD), Arizona	2023, Tangles and Webloc 2023 - 2025, Tangles
Durham Police Department, North Carolina	2024 - 2027, Tangles and Webloc
New York City District Attorneys of Queens and Bronx County	2023 - 2025, Tangles and Webloc
City of Elk Grove Police Department, California	2023 - 2028, Tangles and Webloc
Pinal County Sheriff’s Office, Arizona	2022 - 2023, Tangles and Webloc

Table 3: Purchases of Webloc and other Cobwebs products by U.S. state and local customers.

Webloc customers also include police departments and other law enforcement agencies in both larger and smaller cities and counties in California, Texas, Maryland, North Carolina, New York and Arizona.

Los Angeles Police Department

The Los Angeles Police Department (LAPD) entered into a one-year Tangles and Webloc contract in 2022, as initially reported by *Knock LA*, which obtained documents via freedom of information requests. When asked about Webloc, the LAPD stated it uses "commercially available anonymized data in relation to criminal investigations." A LAPD report, which does not distinguish between Tangles and Webloc, states that the Cobwebs system was used by the Robbery-Homicide Division (RHD) and Major Crimes Division (MCD), and it had been queried 136 times in 2022 and 1,319 times in 2023. We consider LAPD a confirmed Webloc customer from 2022 to 2023.

Dallas Police Department

Dallas Police Department (DPD) has been a Webloc customer at least in 2025, according to a statement DPD provided to the Dallas Observer.[28] Public records show that the City of Dallas authorized a three-year purchasing agreement for Cobwebs software worth $303,963 in January 2025. DPD claims that Webloc is not "not widely used" in the department. The system is used by DPD's Fusion Center, according to a city council member. We consider Dallas police a confirmed Webloc customer in 2025 and a potential Webloc customer until 2028.

Baltimore County Police Department

The Baltimore County Police Department purchased Webloc in 2022 on behalf of its Crime Strategies and Analysis Division in order to "properly plan for public safety issues and events," according to public records. In 2024, it entered a three-year Tangles and Webloc contract subject to annual renewals. In 2021, Baltimore County purchased an annual license representing a "continuation of a subscription" for the "Cobwebs Technologies Web Investigation Platform" Tangles, and it had a supplier contract with Cobwebs Technologies also between 2023 and 2024. We consider Baltimore County police a confirmed Webloc customer from 2022 to 2024 and a potential Webloc customer for the entire period from 2020 to 2027. This was not reported to our knowledge.

[28] DPD stated in 2025 that Webloc is available but "not widely used": https://www.dallasobserver.com/news/dallas-pd-renews-contract-with-controversial-surveillance-platform-21571528

Tucson Police Department

In August 2023, Tucson Police Department (TPD) entered into a 28-month Tangles contract, as first reported by the *Arizona Mirror* based on a document obtained via a freedom of information request. The document, which represents a reimbursement request sent from TPD to the State of Arizona, contains a report that provides an overview of how the system was used in 2023. As TPD used “advertisement identification numbers” to “identify unique identifiers of cellphones” we conclude that Webloc was purchased at least in 2023. In 2025, it told the Arizona Mirror that it does not have access to Webloc under its current contract. We consider Tucson police a confirmed Webloc customer in 2023 and a potential Webloc customer in 2024.

Case Study I: Disproportionate Use and Mission Creep

Tucson police explained in an internal report that Tangles and Webloc were “purchased for sex trafficking investigations” but readers “will see it has applications that span across the agency."

Example cases presented in the report include the use of Webloc to investigate burglary, robbery, and theft of “thousands of dollars of cigarettes." Tucson police used the system to search for "advertisement identification numbers" of phones that were present in areas where a series of thefts and burglaries occurred, according to the report. It identified a bar where the suspect was employed, a woman who turned out to be the suspect’s former girlfriend and an “apartment address that the phone identifiers kept ending up at after each crime."

The system was also used to monitor protests during visits of presidential and vice-presidential candidates. The purchase was paid for with money from Arizona’s Border Security Fund.

While the system was purchased for border security purposes and sex trafficking investigations, it was used for routine criminal cases with damages of a few thousand dollars and for monitoring protests.

Durham Police Department

The police department of the city of Durham, North Carolina, entered into a three-year Tangles and Webloc contract in 2024, according to a publicly available contract[29] including a quote[30] that refers to both Tangles and Webloc being part of the contract. While the contractual document is not signed, the city council authorized the purchase. We consider Durham Police Department a confirmed Webloc customer 2024 to 2025 and a potential Webloc customer from 2026 to 2027. This was not reported to our knowledge.

Elk Grove Police Department

In 2023, the police department of the City of Elk Grove, California, entered into a five-year Tangles and Webloc contract, according to documents obtained by EFF via a freedom of information request. The documents also include invoices and payment confirmations for the annual renewal in 2024. A city council record suggests that the system is used by Elk Grove police's "Real-Time Information Center (RTIC)" to investigate crimes and "proactively provide leads in developing new investigations" including for "sex trafficking and organized retail theft investigations." We consider the Elk Grove Police Department a confirmed Webloc customer from 2023 to 2025 and a potential Webloc customer until 2028.

NYC District Attorneys of Queens and Bronx

The New York City district attorneys of Queens and Bronx counties purchased one-year Tangles and Webloc licenses in 2023 and 2024, according to public notices and hearing records.[31]

Sheriff's Office of Pinal County

The Sheriff's Office of Pinal County, Arizona, paid around $90,000 for Tangles and Webloc in 2022 and 2023, according to the *Texas Observer* and statements provided by the Sheriff's Office. A spokesperson told the Texas Observer that he has "not surveyed our handful of users, but one of our analysts just told me he has only used it a few times" and added that "no warrant was obtained."

---

[29] https://cityordinances.durhamnc.gov/OnBaseAgendaOnline/Documents/DownloadFile/Final-Published%20Attachment%20-%2017404%20-%20CONTRACT%20-%20-%202%20-%20PENLINK%20CONTRACT%20-%201.pdf?documentType=1&meetingId=673&itemId=41500&publishId=232800&isSection=False&isAttachment=True, accessed 14.10.2025

[30] https://cityordinances.durhamnc.gov/OnBaseAgendaOnline/Documents/DownloadFile/Final-Published%20Attachment%20-%2017404%20-%20PRICE%20QUOTE%20-%203%20-%20QUOTE%20-%2012_16_2024.pdf?documentType=1&meetingId=673&itemId=41500&publishId=232801&isSection=False&isAttachment=True, accessed 14.10.2025

[31] https://mspwww-dcscpfvp.nyc.gov/RequestDetail/20230828102, https://a856-cityrecord.nyc.gov/RequestDetail/20231113021, https://a856-cityrecord.nyc.gov/RequestDetail/20240930102, https://a856-cityrecord.nyc.gov/RequestDetail/20230406118, https://www.nyc.gov/assets/dcas/downloads/pdf/cityrecord/2024/cityrecord-05-06-24.pdf, accessed 17.3.2026

Case Study II: Warrantless Surveillance at the Texas/Mexican Border

A comprehensive investigation by the Texas Observer published in 2026 by Francesca D'Annunzio discusses how Webloc was used for warrantless surveillance at the Texas-Mexican border, based on interviews with Roy Boyd, sheriff of Goliad County, Texas, and his deputy.

Boyd told the Texas Observer that, using Webloc, a police analyst discovered six phones that were tracked at both an immigration checkpoint and a store associated with a receipt, which was found when his police unit was investigating the driver of a vehicle that was suspected of carrying undocumented immigrants but could not be identified via the licence plate. Boyd did not say whether these leads led to an arrest. A corresponding incident retrieved by the journalist via a records request does not mention Webloc but states that the police collaborated with a Homeland Security Investigations analyst. The Texas Observer cites from interviews with Boyd and his deputy who stated, as summarized by the journalist, that the "tracking software doesn't reveal names, only device identification numbers in the online advertising ecosystem." The data was "sourced from applications in which consumers consented to sharing their whereabouts."

We did not find any public records that would clarify whether Goliad County itself purchased Webloc or accessed resources from other agencies. According to the *Texas Observer*, Goliad County sheriff Boyd leads a task force named after Texas governor Abbott's border militarization mission "Operation Lone Star," which pools resources from nearly 60 Texas agencies including CBP and ICE. The investigation found that "nearly 20 Texas sheriff's offices have obtained a Tangles log-in." When the Texas Observer was reaching out to 80 public defender offices and a network of more than 60 immigration attorneys, no one provided any examples of Tangles being mentioned in court records. An ACLU attorney cited in the article concluded that either the technology would be "a massive waste of taxpayer money" or they are "hiding it from judges, criminal defense attorneys, criminal defendants and the press."

Hungary

In collaboration with *VSquare*, we reveal the Hungarian government as a Webloc customer. Alongside our report, investigative journalist Szabolcs Panyi published a report in *VSquare* which shows that Hungarian domestic intelligence has used Webloc and other products developed by Cobwebs Technologies since at least 2022. In March 2026, a new set of licenses including Webloc was purchased. Panyi's investigation is based on primary documents shared with him and several anonymous sources who asked not to be named. We reviewed a partial selection of these documents.

According to *VSquare*'s findings, at least three Hungarian civilian intelligence agencies have been using Cobwebs products. This includes the domestic intelligence agency Constitution Protection Office (AH), the data fusion agency National Information Centre (NIC), and the Special Service of National Security (NBSZ), which performs surveillance operations on behalf of other agencies. All three agencies - AH, NIC and NBSZ - are overseen by the Cabinet Office of the Hungarian Prime Minister.

The newest round of licenses was purchased by the NBSZ in March 2026. According to *VSquare*'s findings, it includes dozens of licenses for Tangles, almost two dozen for CoAnalyst, six for Webloc, a few for a blockchain analysis module, and less than ten for what is listed in the procurement records as "Full AI." The "Full AI" package is understood to refer to the AI-enhanced add-ons - facial recognition, natural language processing, and automated insight generation - bundled as a single upgrade to the Tangles platform. The NBSZ distributes the tools to partner agencies across the Hungarian intelligence and law enforcement community, according to *VSquare*.

VSquare reports that a broker company, SCI-Network, sold the licences to the Hungarian government in March 2026 and suggests that SCI-Network is led by a person with close ties to Antal Rogán, the chief of the Hungarian Prime Minister's Cabinet Office. Purchasing the tools through SCI-Network as broker, is reported as having inflated the cost of the licences by as much as 100% compared to direct procurement of the products. SCI-Network are also reported as developing their own "zero-click" spyware tool capable of targeting mobile phones.

To our knowledge, the Hungarian Webloc purchase represents the first confirmation of the use of ad-based surveillance technology in Europe. While reports from European think tanks and intelligence oversight agencies have previously suggested that several E.U. member states may have purchased commercially available data for surveillance purposes, the European public has so far been kept in the dark about the procurement of specific ad-based surveillance products by specific national authorities.

VSquare's findings on the Hungarian Webloc purchase suggest that the Hungarian government purchased a system that may rely on large amounts of personal data unlawfully processed by an ad-based surveillance vendor and its data sources including mobile app vendors and other parties that help distribute the data. In Europe, the processing of personal data and its sharing with third parties is governed by the General Data Protection Regulation (GDPR). As discussed in **Section 10**, the safeguards implemented by the GDPR make it unlikely that mobile apps can lawfully share data originally processed

for purposes such as operating consumer apps or displaying digital advertisements with third parties who used it for an entirely different purpose – namely, government surveillance. We encourage the Hungarian Data Protection Authority, which is responsible for enforcing the GDPR in Hungary, and other European GDPR regulators, to investigate the lawfulness of data processing by ad-based surveillance and their data sources.

The deployment of ad-based surveillance technology in Hungary is especially troubling. Hungary, with national elections scheduled for April 12, 2026, is facing renewed pressure to uphold its international human rights obligations and to reverse its crackdown on dissent. On April 1, 2026, the Council of Europe released a statement saying that "Hungary's elections must not be shaped by fear, abuse of state resources or foreign manipulation," and revealed that the delegation of election observers who had travelled to Budapest to monitor the elections had "pointed to a toxic climate marked by the blurring of state and party, the massive use of all state and government resources in favour of one party, a distorted information space, inflammatory propaganda, captured institutions, growing concern over foreign malign interference and hostility towards independent civil society organisations."

On March 26, 2026, while Szabolcs Panyi was collaborating with the Citizen Lab on this project, it was announced by the chief of staff to the Prime Minister Viktor Organ that the government had filed criminal charges against Panyi for espionage. The charges relate to an investigation by Panyi about Russian influence operations ahead of the country's parliamentary elections. On April 1, 2026, the Committee to Protect Journalists called on the Hungarian authorities to immediately drop the charges and to ensure that journalists can operate in Hungary without intimidation or threats of imprisonment.

Hungary's use of surveillance technology has been widely reported. In 2021, the Citizen Lab in collaboration with the Pegasus Project revealed that Hungary had purchased NSO's group's Pegasus spyware and had used it to target citizens, journalists, lawyers, and opposition politicians. According to *VSquare*'s report, multiple sources with knowledge of the Hungarian intelligence community are concerned about the potential use of surveillance technologies developed by Cobwebs Technologies to monitor opposition figures and journalists, particularly given the absence of judicial oversight of intelligence collection in Hungary.

El Salvador

The National Civil Police (PNC) of El Salvador purchased Tangles, Lynx, and Webloc in December 2020, according to an investigation by the El Salvadoran media outlet *El Faro* and leaked documents we obtained from a source. National Civil Police spent $680,000 USD on the contract awarded to Eyetech Solutions, a Mexican reseller of Cobwebs Technologies products.

One of the leaked documents titled "Technical Proposal" sets out what Eyetech Solutions offered to the National Civil Police, including Tangles, Lynx, and Webloc. As detailed in **Section 3**, it describes the capabilities of Webloc. Deliverables include the installation of the system and training on Tangles, Lynx, and Webloc.

According to the *El Faro* investigation, Tangles, Lynx and Webloc were used from at least January 2021 until January 2022. Despite our attempts to locate follow-up contracts, we have not found any to date, though their existence cannot be ruled out.

The use of ad-based surveillance technology in El Salvador is particularly concerning given the well-documented pattern of state repression against civil society, independent media, and political dissent. Since 2021, the Bukele government has systematically dismantled democratic checks and balances and established a permanent state of exception, under which more than 89,000 people have been arbitrarily detained, with widespread reports of torture, forced disappearances, and deaths in custody.[32] Human rights organizations, journalists, and political opponents have been specifically targeted. For example, between 2020 and 2021, at least 22 staff members of the investigative outlet *El Faro* were surveilled using Pegasus spyware, as confirmed by the Citizen Lab. Organizations such as Cristosal, which has documented hundreds of abuses under the state of exception, have faced stigmatization campaigns, illegal surveillance, judicial harassment, and legal obstruction of their work. Independent oversight has been neutralized, judicial independence captured, and dissent criminalized.[33]

5. Potential Webloc Customers

To identify additional Webloc customers, we analyzed existing media reporting, carried out systematic research on the web, and searched public records about government purchases in several countries. According to our research about Webloc customers in the U.S., Webloc is sold almost exclusively as an add-on product to the social media and web intelligence system Tangles. As such, our investigation aimed to identify both Tangles and Webloc customers.

The use of ad-based surveillance technology by government agencies, including the use of Webloc, is well documented in the U.S., as shown in the previous section. Since we know little about the use of these technologies in other regions in the world, including Europe, this section focuses on potential Tangles and Webloc customers outside of the U.S. The analysis of server infrastructure associated with Cobwebs products contributes to our understanding of the countries and regions where Tangles and Webloc customers may be located.

To identify potential Webloc customers in Europe and the U.K., where the use of personal data from mobile apps and digital advertising is regulated by the GDPR and the U.K. GDPR, we sent 96 Freedom of

[32] International Group of Experts for the Investigation of Human Rights Violations in the Framework of the State of Emergency in El Salvador (GIPES), El Salvador en la encrucijada: crímenes de lesa humanidad bajo la política de seguridad pública (March 2026); CIDH, Informe Estado de excepción y derechos humanos en El Salvador, OEA/Ser.L/V/II, Doc. 97/24 (June 28, 2024).

[33] DPLF, Justicia Amordazada: La captura del sistema de justicia en El Salvador (July 13, 2022); WOLA, Reformas electorales en El Salvador allanan camino para mayor consolidación del poder (March 23, 2023).

Information (FOI) requests spanning 14 countries and 6 European Union institutions. On the whole, we directed our FOIs to departments responsible for law enforcement and immigration.

While several departments confirmed that they do not use Webloc, others refused to provide information citing law enforcement or national security exceptions. Not one government agency confirmed their use of Webloc (and many did not respond at all).

As part of our research, we asked government agencies about their use of a number of different ad-based surveillance products, sent in separate requests. In some cases, a government department confirmed they did not use a specific ad-based surveillance product (other than Webloc), but refused to answer the question specifically about access to Webloc. We believe that such ambiguous responses suggest that the government department in question may actually have access to Webloc and should be further investigated.

United Kingdom

We sent FOI requests asking about access to Webloc to 44 individual police forces in the U.K. and received responses from all. Five of the 44 police forces confirmed that they did not hold information relevant to our request (and did not have access to the product), 39 of the police forces said they could not confirm nor deny whether they had access to Webloc because to do so would impact their law enforcement capabilities and negatively impact national security. One police force, Gwent Police, confirmed they did hold relevant information relating to our request and that they were performing an assessment as to whether they could disclose the information. They later sent a contradictory response claiming they could neither confirm nor deny whether they held the information.

Through further FOI requests, we received confirmation that the U.K.'s controversial National Police Chiefs' Council (NPCC) Central Referral Unit (CRU) provided police forces across the country with a standardized response to our requests. This unit has been criticized for preventing police transparency and acting as a 'censor'. We believe that the fact that some police forces were able to confirm that they did not have access to Webloc, while others were not able to respond for law enforcement reasons, potentially suggests that at least some police forces in the U.K. have access to Webloc. We recommend further investigation into the use of Webloc by police forces in the U.K.

We also sent a FOI request to the U.K.'s Home Office asking about their access to Webloc. We received a response from the Immigration Enforcement unit within the Home Office saying that they could neither confirm nor deny whether they had access to Webloc due to law enforcement and national security reasons. We also asked the Home Office whether they had access to other ad-based surveillance products developed by competitor vendors Babel Street, Shadow Dragon, Rayzone, Insanet, and Intelos. For each of these vendors and products, the Home Office confirmed that they did not hold relevant information or have access to the products. We believe this also strongly suggests that the Home Office has had access to Webloc. We appealed the Home Office's response to our FOI to the Information Commissioner's Office (ICO) in July 2025. The Home Office submitted materials to the ICO 'in

confidence' in response to our appeal, requesting that the information be kept confidential and not disclosed to the public or to Citizen Lab. Our appeal was ultimately denied by the ICO in February 2026. In light of these FOI responses, we recommend further investigation into the Home Office's use of Webloc.

Cobwebs products are available for purchase in the U.K. via the U.K. government's digital marketplace (an online platform where public sector organizations can find and buy digital services). Penlink appears in the marketplace as a 'vetted supplier' for the procurement framework that runs from October 29, 2024, to October 28, 2026. Although Penlink Technologies is the listed supplier, all the procurement materials on the U.K. government marketplace for products supplied by Penlink are Cobwebs branded, including the pricing document and the terms and conditions.

Cobwebs materials also describe a "dedicated education centre in central London" and state that "UK datacentres are used for UK clients." The Penlink website shows that there is dedicated Tangles support in the U.K. There is also a U.K.-based subsidiary, "Pen-Link Technologies UK Ltd." According to company information, Omri Timianker, the founder of Cobwebs, is a director of Pen-Link Technologies UK Ltd.

Based on technical analysis,we identified seven active servers located in the U.K. that we consider to be associated with Cobwebs product deployments.

Europe

Austria

Procurement records show that the Austrian Federal Ministry of the Interior (Bundesministerium für Inneres) bought Tangles in December 2024 for 847,000 Euro. The name of the supplier was anonymized in the procurement records. We sent a FOI request to the authorities to ask if the government had purchased Webloc as part of this contract. They refused to confirm or deny whether they held any information citing the need to maintain public order and security. A comprehensive parliamentary inquiry on the matter was rejected with similar arguments, but referred to a specific subcommittee that would exercise parliamentary oversight for the domestic intelligence agencies while maintaining confidentiality.

Other FOIs. We also sent freedom of information requests to different government departments in France, Netherlands, Italy, Poland, Belgium, Denmark, Sweden, Greece, Romania, and Bulgaria, asking whether they had purchased Webloc. We received no responses to our requests from Greece, Belgium, Italy, France or Bulgaria. We received the following responses:

- **Netherlands**: The Ministry of Defence refused to provide the information citing national security reasons (we received no response from the Ministry of Justice and Security or the Ministry of Asylum & Migration).

- **Sweden**: The Swedish Police Authority said they would not provide the information for law enforcement reasons. They did confirm, however, that they do not use Babel Street products. Other government departments in Sweden, namely the Ministry of Justice, Swedish prosecution authority and Swedish Commission on Security and Integrity Protection, confirmed they have not purchased Webloc.
- **Romania**: The General Inspectorate for Immigration refused to provide the information stating they are not required to do so by law.
- **Poland**: The National Police confirmed they have not purchased Webloc (we received no reply from the Central Anti-Corruption Bureau).
- **Denmark**: Four government departments in Denmark confirmed they have not purchased Webloc.

We also sent requests to the following E.U. institutions: Europol, Eurojust, European Public Prosecutor's Office, European Anti-Fraud Office, Frontex, and the European Defence Agency. All except for Europol confirmed that they do not have any documents relating to the purchase or use of Webloc.

Europol

Europol confirmed that they do have documents related to their access to the Cobwebs product Tangles and Webloc. They listed the documents as follows:

1. EDOC #1278947 (March 2023)
2. EDOC #1366842 (January 2024)
3. EDOC #1361494 (February 2024)
4. EDOC #1432425 (February 2025)
5. EDOC #1447455 (February 2025)
6. EDOC #1441679 (February 2025)

We then asked Europol to disclose the contents of those documents, or at least provide partial access, such as the titles of the documents. They refused to do so, citing protection of public interest and commercial interests. We appealed that decision and that appeal was denied. Europol was able to confirm, however, that they did not have access to other ad-based surveillance products produced by Babel Street and Rayzone.

At a conference panel hosted by Computers, Privacy and Data Protection (CPDP) in May 2025 on the subject of "Advertisement Intelligence by European Agencies," a senior data protection supervisor at Europol mentioned that his colleagues had presented him with a quote from a commercial intelligence provider based in Israel and asked his opinion if they could purchase it. He described the intelligence provider's quote as saying "we will get you any information you need. So we will infiltrate, we will impersonate, we will hack into the system. Whatever it is you need, we will make sure you get it." After

studying the quote and the included terms and conditions, the data protection supervisor claimed that Europol's data protection office stopped the procurement from going ahead.

Germany

A parliamentary inquiry asking the German federal government about whether it uses Webloc or other specific ad-based surveillance products was rejected, as reported by *netzpolitik.org*. The inquiry excluded German intelligence agencies. The government refused to answer the parliament's questions also for federal police forces citing national security reasons. The government however stated that the acquisition of personal data from data brokers can be appropriate in some cases.

Additional Research on European Countries

We found other information suggesting that Tangles, Webloc or other Cobwebs products are being sold in Europe countries:

- **Italy:** The Local Police of Venice hosted a Tangles and Webloc training day in July 2022, which suggests that Webloc has been in use in Italy at least for a brief time period. We are not aware of any information that clarifies whether Venice police conducted any assessment of the legal implications ahead of the event.
- **Netherlands:** The Dutch company, DataExpert, is a reseller of Cobwebs products in Europe and specifically advertises Webloc capabilities claiming that "Cobwebs lets you... use integrated ADINT (Advertisement Intelligence) functionalities." European public procurement records show that DataExpert sold a number of software products in Europe between 2016 to 2026, including in Denmark, Belgium, and the Netherlands (the records do not state what product they sold to these governments).
- **Germany:** Cobwebs Technologies has a corporate entity registered in Germany since 2019. At some point, it was renamed from "Cobwebs GmbH" to "PEN-LINK GmbH." Omri Timianker is listed as a director.[34] It has also been reported that Cobwebs had a sales representative based in Germany who was previously a sales representative at NSO Group.
- **Spain:** The Spanish company, Ondata International, is also a reseller of Cobwebs products. Procurement records show that they have sold a number of software products to Spain and Portugal in the last few years (the records do not suggest what product they sold).
- **France:** Cobwebs' promotional materials, and subsequent reporting in the French press, suggest that the French police used Tangles to monitor audiences at the Atletico Madrid versus Marseille FC Europa League Final in 2018.

Based on technical analysis detailed below, we identified active servers located in the Netherlands (32), Germany (8), France (2), Ireland (1), Sweden (1), Norway (1), and Cyprus (1) that we consider to be associated with Cobwebs product deployments. The Netherlands appear to be a major node in Cobwebs

[34] https://www.northdata.com/Pen-Link%20GmbH,%20M%C3%BCnchen/Amtsgericht%20Frankfurt%20am%20Main%20HRB%20117403, accessed 18.3.2026

server infrastructure. One of the servers located in the Netherlands might be associated with a Webloc deployment, as detailed in **Section 6**. In our analysis, we found additional hosts which we consider to be associated with the wider Cobwebs server infrastructure located in Hungary, Poland, and Italy.

United States

Department of Homeland Security (DHS)

While ICE is a confirmed Webloc customer, as discussed in the previous section, other DHS components may have also purchased it. Customs and Border Protection (CBP) was a Tangles customer at least in 2024[35] and it has utilized ad-based location data at least from 2019 to 2021, according to a document released by the agency. The DHS also purchased annual Tangles licenses in 2024 and 2025 in "support" of its "insider threat program." A notice related to the 2024 contract discusses "commercially available information" and "geo location data." Monitoring "insider threats" typically involves monitoring an organization's own employees. Another DHS component, the Office of Intelligence & Analysis (I&A), entered into a five-year Tangles contract worth up to $3 million in 2020 and used the system to compile dossiers on protesters, according to an internal DHS report. We consider CBP and the DHS' insider threat program as potential Webloc customers.

Other Federal Customers

Additional federal Tangles customers in the U.S. include the Department of Justice (DOJ), the Department of Energy, and the Internal Revenue Service (IRS).

State-Level Law Enforcement

State-level law enforcement departments who purchased Tangles include the Vermont Department of Public Safety[36], Illinois State Police,[37] New York State Police,[38] Colorado Department of Public Safety,[39] Hawaii State Fusion Center[40], and the District of Columbia's Homeland Security and Emergency Management Agency (HSEMA). North Carolina's State Bureau of Investigation (SBI) also used Cobwebs

[35] "The Tangles SaaS platform ... is currently employed by DHS CBP," DHS notice, Jul 19, 2024. Available at: https://sam.gov/opp/3073affc533f4741abc6e42f93957cb0/view, accessed 24.3.2026

[36] https://data.vermont.gov/Finance/Executed-Contracts-for-Service/dz5q-8uqb/about_data, https://data.vermont.gov/Finance/Vermont-Vendor-Payments/786x-sbp3/data_preview, accessed 24.3.2026

[37] https://www.bidbuy.illinois.gov/bso/external/bidDetail.sdo?docId=26-493ISP-OPERA-B-48979, accessed 24.3.2026

[38] https://www.muckrock.com/foi/new-york-16/cobwebs-contracts-161816/, accessed 24.3.2026

[39] https://prd.co.cgiadvantage.com/PRDVSS1X1/Advantage4, accessed 14.10.2025

[40] https://hiepro.ehawaii.gov/resources/160885/HSFC Contract Requirement HIEPRO 05202025.pdf, accessed 24.3.2026

software.[41] The Connecticut Judicial Marshall Services purchased "Threat Intelligence Software" from Cobwebs Technologies.[42] A notice related to the contract explained that Judicial Marshall Services aimed to use the system to monitor "potential civil unrest" and "subversive groups" in the context of threats against judges and employees.

Local Law Enforcement

A quote for a Tangles contract of San Joaquin Sheriff's Office in California includes an option for "Webloc Geo source data," according to documents obtained via a freedom of information request, which was only made available after the Electronic Frontier Foundation (EFF) went to court. While the Webloc option is not visible in the corresponding purchase order, we still consider the sheriff's office of San Joaquin a potential Webloc customer. We also consider the police department of Amarillo in Texas a potential Webloc customer, as it considered buying Tangles including the "ability to access, search and analyze mobile device communication records," according to a city council memo.

As discussed in the previous section, the sheriff of Goliad County, also in Texas, discussed the use of Webloc in an interview while leaving it unclear whether his office had purchased the system by itself or accessed external resources. Several other police units in counties and cities in the U.S., both large and small, have purchased Tangles, including the police departments of Hartford,[43] Houston, Winston-Salem,[44] Panama City Beach, and Prince George's County and the sheriff departments of LA County, Henry County[45], and Jackson County.[46] A Texas Observer investigation found that "nearly 20 Texas sheriff's offices have obtained a Tangles log-in."

As information about such contracts is sparse and sometimes difficult or impossible to access, we assume that additional state and local agencies and departments other than the ones listed have purchased Tangles and Webloc.

---

[41] "Cobwebs is currently being used by other law enforcement agencies, to include the North Carolina State Bureau of Investigation," City of Raleigh memo, March 1, 2024. Available at: https://go.boarddocs.com/nc/raleigh/Board.nsf/files/D39MTA5A2AC5/$file/20240319RPDDonationAcceptanceRequest.pdf, accessed 25.10.2025

[42] https://www.jud.ct.gov/BidPortal/PublicBidInfo.aspx?Bid_ID=13145&m=Vendor, accessed 24.3.2026

[43] https://www.muckrock.com/foi/hartford-97/foia-cobwebs-technologies-hartford-police-department-130326/, accessed 24.3.2026

[44] "Winston-Salem PD has been utilizing the platform since July 2023," "IT Governance Business Case," City of Durham, Jun 6, 2024. Available at: https://issuu.com/cityofdurham/docs/cobwebs_web_investigation_platform_-_police.pptx, accessed 14.10.2025

[45] https://www.muckrock.com/foi/henry-county-4907/open-records-request-cobwebs-materials-173651, accessed 24.3.2026

[46] https://www.co.jackson.tx.us/upload/page/2342/docs/Financial/Budgets/Budget%20FY2024_ADOPTED%20to%20POST_20230905.pdf, accessed 28.10.2025

Other Regions

Mexico

Several authorities in Mexico have acquired Tangles licenses through Karsos S.A. de C.V. including the Mexico State prosecutor office, Mexico City's prosecutor office, and the State of Jalisco. A media investigation suggests that Webloc might have been included in one of the contracts in Mexico. In 2021, the Cobwebs website listed an office in Mexico. Based on technical analysis,we identified two active servers located in Mexico that we consider to be associated with Cobwebs product deployments. As detailed in **Section 6**, one of the two servers might be associated with a Webloc deployment.

Colombia

Several documents confirm that Colombia's public prosecutor office, Fiscalía General de la Nación (FGN) acquired licenses for Tangles. A report by the organization "Fundación Karisma" mentions a contract with "Desarrollo e Integración de Tecnología y Comunicaciones S.A.S. (Deinteko SAS)" with the purpose of "updating licence for Tangles platform." Recent public financial statements of FGN confirm a new contract in 2024 with Deinteko for the "update and technical support of 8 Tangles licenses." Based on technical analysis, we identified one active server located in Colombia that we consider to be associated with a Cobwebs product deployment.

Vietnam

Since at least 2024, a Vietnamese reseller has offered the Cobwebs products Tangles, Webloc, and Lynx on its website. In addition, we discovered a Vietnamese Cobwebs-branded "Technical specifications" document dated 2021 on the web.[47] The document appears to provide detailed contractual requirements for the deployment of a 'WEBINT' system including the Cobwebs products Tangles, Lynx, Trapdoor and Webloc. The requirements listed in the document are very specific. For example, it states that the party implementing the Cobwebs system must have current deployments on Microsoft Azure Cloud in the Asia-Pacific region. The document might be related to a contract or it may represent merely a contractual template. The existence of a Vietnamese Webloc reseller, combined with a Vietnamese document that contains technical specifications for a Webloc deployment, raises the need for further research into potential Webloc customers in Vietnam.

Singapore

Cobwebs has had a corporate entity named "Cobwebs Asia Pte Ltd" registered in Singapore since 2017. The website of an entity named "CWA Webint Applications," whose offerings match the descriptions of Tangles, Lynx and Trapdoor, shares the Singapore postal address displayed on the site with the

[47] Accessed on 12.3.2026 and archived by the authors: https://www.studocu.vn/vn/document/hoc-vien-cong-nghe-buu-chinh-vien-thong/ki-thuat-lap-trinh/7-webint-specifications/118733920, accessed 12.3.2026

registered address of Cobwebs Asia Pte Ltd. Based on technical analysis, we observed a server that we consider to be associated with a Cobwebs product deployment displaying a login page, whose design matches the design of Tangles login pages. We believe that CWA is either closely affiliated with or identical to Cobwebs. Overall, we identified 17 servers located in Singapore that we consider to be associated with the deployment of Cobwebs products. As detailed in **Section 6**, two servers might be associated with Webloc and Trapdoor deployments. The current PenLink website offers "Tangles Product Support" in Singapore.

New Zealand

In New Zealand, a 2022 report revealed that the Ministry of Business, Innovation and Employment (MBIE) had been using Cobwebs technology since 2019 to monitor all major platforms to "covertly collect people's personal data." The report states that it delivers this data to analysts in the MBIE Intelligence Unit, which is part of Immigration New Zealand. A later report in 2024 by the same publication said that documents obtained by FOIs revealed that the intelligence unit had been questioned by watchdogs over their use of Cobwebs products and that the government admitted that "Cobwebs was bought to combat mass arrivals of asylumseekers [sic] by boat." In 2024, an "automated register of false personas to use on social media platforms" was set up, according to documents obtained via a FOI request. This information suggests that the New Zealand government might have purchased not only Tangles, but also Lynx.

Israel

While Cobwebs Technologies has long been headquartered in Israel, we are not aware of confirmed product deployments in the country. According to records on LinkedIn, three Israeli military personnel received Webloc training in 2022 and 2024 while working for the Israeli Defence Forces.[48] We identified 37 hosts located in Israel that we consider to be associated with the company's server infrastructure.

Other Countries

We found information about the presence of Cobwebs products in additional countries. The 2021 version of the company's website displayed offices in Indonesia and India. The current PenLink website offers "Tangles Product Support" in Thailand and Australia. Based on technical analysis, we identified active servers that we consider to be associated with Cobwebs product deployments located in Indonesia, Hong Kong, Japan, United Arab Emirates, Iraq, and Kenya. We identified an additional host in Brazil that we consider to be associated with Cobwebs Technologies' server infrastructure.

Microsoft Offerings

While not a potential Webloc customer itself, Microsoft listed Webloc as a "preferred solution" on its AppSource app store in 2022, which allowed customers to find, try, buy, and deploy the listed software.

[48] https://www.linkedin.com/in/yoav-shabat/; https://www.linkedin.com/in/eden-kaziev-65189428a/; https://www.linkedin.com/in/rami-madi-2303b525a/, accessed 5.3.2026

According to Microsoft, preferred solutions were “selected by a team of Microsoft experts” and come from “Microsoft partners with deep, proven expertise and capabilities to address specific customer needs." Webloc was removed from the app store at some point after 2022. A press release from Cobwebs Technologies published in 2019 suggests that “the company has been working with leading cloud providers, such as Microsoft” since at least 2019.

At the time of publication, Microsoft still lists several products developed by Cobwebs Technologies on its app store, now renamed Microsoft Marketplace, including Tangles, Tangles API, Lynx, Weaver, and Threat Intelligence Solution. Technical analysis suggests that 219 out of the 298 active hosts affiliated with Cobwebs Technologies' server infrastructure are hosted in data centers related to Microsoft's Azure cloud.

6. Cobwebs Server Infrastructure

After receiving a tip about Cobweb's infrastructure from colleagues at Amnesty International’s Security Lab, we mapped out server infrastructure that we consider to be associated with deployments of Cobwebs products in at least 21 countries.

Our technical analysis identifies domains, subdomains, and other web hosts that we consider to be associated with Cobwebs Technologies using common DNS telemetry and IP geolocation tools, the URL telemetry tool Censys, and browser testing. We accessed only publicly available resources without any modification or circumvention of access controls.

Cobwebs Domains and Login Pages

First, we identified three domains affiliated with Cobwebs’ server infrastructure.

The domain cobwebsapp.com is linked to a SSL certificate registered by Cobwebs Technologies using the address of its Israeli corporate entity.[49] The domains cwtapp.com and cwsystem.com are not directly linked to an entity. Common DNS telemetry tools observed 520 subdomains for these three domains, 284 of them resolving to particular IP addresses as of January 30, 2026.

When we viewed the active subdomains in the web browser, 81 of the cwtapp.com subdomains and 35 of the cwsystem.com subdomains displayed a login page containing a Tangles logo, as of March 6, 2026.

Domain	Number of subdomains	Subdomains resolving to IP	Subdomains with active Cobwebs login page
cobwebsapp.com	135	74	-

[49] Certificate information: C=IL, postalCode=46725, L=Herzliya, street=3 Shenkar Arie, O=Cobwebs Technologies, CN=*.cobwebsapp.com

cwtapp.com	155	99	81
cwsystem.com	230	111	35
	520	**284**	**115**

Table 4: Cobwebs-affiliated domains and subdomains.

With a few exceptions, the 115 Cobwebs login pages we observed when viewing cwtapp.com and cwsystem.com subdomains in the web browser look identical (screenshot on the left below). A few login pages were colored orange rather than blue, and one page showed the logo of 'CWA Webint Applications' while looking identical otherwise.[50]

Figure 11: Screenshots of login pages

Tangles Servers

Combining browser testing with an analysis of subdomain naming schemes, we conclude that 205 out of 284 currently resolving subdomains for cobwebsapp.com, cwtapp.com, and cwsystem.com may represent Tangles servers.

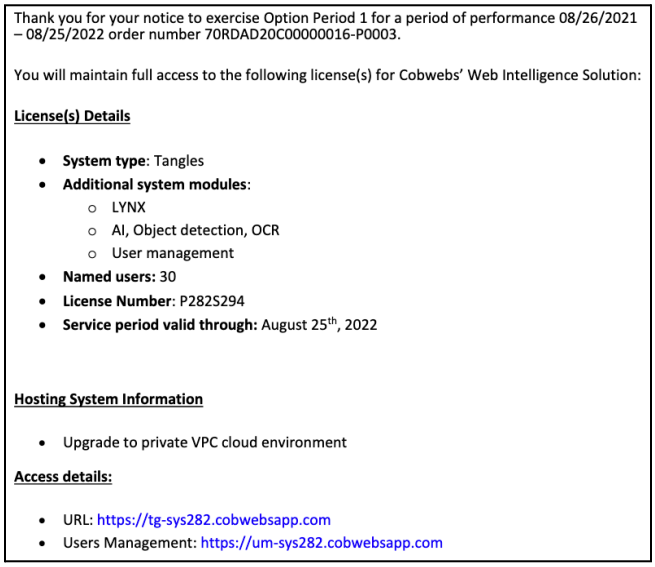
[50] As briefly examined in **Section 5**, CWA Webint Applications appears to be closely affiliated with Cobwebs Technologies.

Domain	Subdomains with particular naming	Examples	Subdomains currently resolving	Subdomains with Tangles login page	Conclusion
cobwebsapp.com	85 subdomain names contain the letters ‘tg’ and a number or acronym	s703-tg.cobwebsapp.com tg-173.cobwebsapp.com tg-zu.cobwebsapp.com	58	0	58 cobwebsapp.com subdomains may represent Tangles servers
cwtapp.com	126 subdomain names contain the letters ‘tg’ and a number	s255-tg.cwtapp.com	81	66	Up to 99 cwtapp.com subdomains may represent Tangles servers
	23 subdomain names contain the letter ‘s’ and a number	s1688.cwtapp.com	18	15	
cwsystem.com	62 subdomain names contain the letters ‘tg’ and a number	p83-tg.cwsystem.com	31	15	Up to 48 cwsystem.com subdomains may represent Tangles servers
	32 subdomain names contain the letter ‘p’ and a number	p07.cwsystem.com p156.cwsystem.com	17	10	
					Up to 205 potential Tangles servers

Table 5: Analysis of potential Tangles servers

As **Table 5** shows, a significant number of subdomain names that contain the letters ‘tg’, ‘s’ or ‘p’, combined with a number or acronym, display a Tangles login page when accessing it in the web browser. We thus consider all subdomains following this naming scheme as potential Tangles servers.

While we were not able to access any cobwebsapp.com subdomain in the web browser, the naming scheme is very similar to the naming scheme observed for many cwtapp.com subdomains. A licensing document related to a contract covering Tangles and Lynx by the U.S. Department of Homeland Security (DHS) from the year 2021, obtained via a freedom of information request, confirms the assumption that subdomains containing the letters 'tg' refer to deployments of Tangles. It also indicates that a subdomain containing the letters 'um' refers to Cobwebs' user management system, which appears to allow a Cobwebs customer to determine who gets access to a system.



Thank you for your notice to exercise Option Period 1 for a period of performance 08/26/2021 – 08/25/2022 order number 70RDAD20C00000016-P0003.

You will maintain full access to the following license(s) for Cobwebs' Web Intelligence Solution:

License(s) Details

- **System type**: Tangles
- **Additional system modules**:
  - LYNX
  - AI, Object detection, OCR
  - User management
- **Named users:** 30
- **License Number**: P282S294
- **Service period valid through:** August 25th, 2022

Hosting System Information

- Upgrade to private VPC cloud environment

Access details:

- URL: https://tg-sys282.cobwebsapp.com
- Users Management: https://um-sys282.cobwebsapp.com

Figure 12: Licensing document related to a DHS contract

We have high confidence in the assessment that subdomains that displayed Tangles login pages are associated with Tangles product deployments. We have medium confidence in the assessment that subdomains that did not display a login page but are following a similar naming scheme are associated with Cobwebs product deployments.

Servers Related to Other Products

A few subdomains appear to refer to other Cobwebs products, 10 of them resolving to particular IP addresses as of January 30, 2026. Subdomains containing the letters 'td' may refer to Trapdoor, subdomains containing the letters 'wr' may refer to Weaver, and subdomains containing the letters 'wl' may refer to Webloc. Subdomains containing the letters 'um' may refer to Cobwebs user management system, as discussed above.

Domain	Subdomain naming scheme	Example subdomains	Interpretation
cobwebsapp.com	14 subdomain names contain the letters ‘um’	s637-um.cobwebsapp.com	29 cobwebsapp.com subdomains may refer to servers related to Trapdoor, Weaver, Webloc and Cobwebs’ user management system, 8 of them currently resolving
	6 subdomain names contain the letters ‘td’	s470-td.cobwebsapp.com	
	4 subdomain names contain the letters ‘wr’	wr-s361.cobwebsapp.com	
	5 subdomain names contain the letters ‘wl’	s704-wl.cobwebsapp.com	
cwtapp.com	1 subdomain name contains the letters ‘um’	s725-um.cwtapp.com	1 cwtapp.com subdomain may refer to a server related to Cobwebs’ user management system, currently not resolving
cwsystem.com	2 subdomain contain the letters ‘um’	p03-um.cwsystem.com	3 cwsystem.com subdomains refer to servers related to Trapdoor and Cobwebs’ user management system, 2 of them still resolving

Table 6: Potential servers related to Trapdoor, Weaver, Webloc and Cobwebs’ user management system

We have medium confidence in the assessment that subdomains containing the letters ‘td’, ‘wr’, and ‘wl’ refer to servers associated with deployments of the Cobwebs products Trapdoor, Weaver, and Webloc.

More Cobwebs Servers and Login Pages

We identified 14 additional servers associated with Cobwebs based on searching for hosts associated with certificates linked to the Cobwebs domains cobwebsapp.com and cwtapp.com with the URL telemetry tool Censys. Most of the 14 hosts were running a web server listening to particular ports, as of 30 January, 2026. When accessing those hosts in a web browser, four of them displayed login pages including logos for Trapdoor, Weaver, and Cobwebs’ user management system. Some of the login masks

appeared to be broken (see below screenshots for examples). Another host displayed an error page containing multiple references to Tangles.

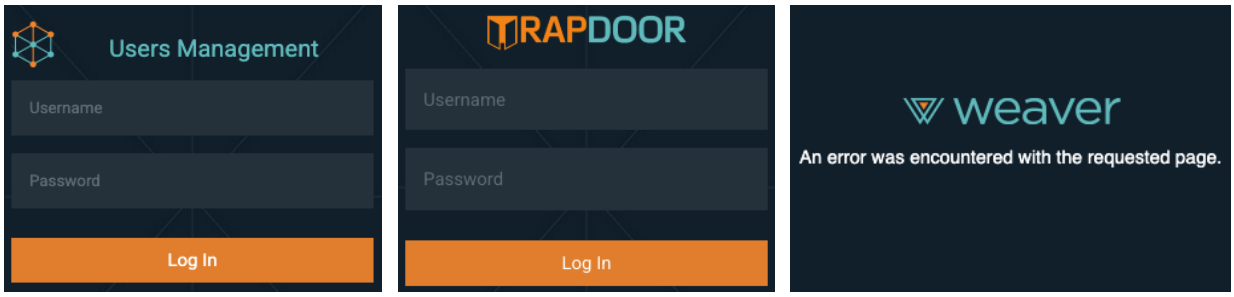


Figure 13: Screenshots of login pages

Cobwebs Server Geolocations

Based on the above research, we identified 219 active servers we assess as associated with Cobwebs product deployments. With the help of common IP geolocation tools we then retrieved the likely server locations of the corresponding IP addresses.

As a result, we found that many potential Cobwebs product servers are located in the U.S. (126), Netherlands (32), Singapore (17), Germany (8), Hong Kong (8), and the U.K. (7). We also identified potential product servers located in Kenya, Iraq, United Arab Emirates, Indonesia, India, Mexico, Colombia, Australia, Japan, and in several European countries (France, Sweden, Norway, Ireland, and Cyprus). We found only one potential product server located in Cobwebs Technologies' home country, Israel.

Country	Potential product servers	All servers
U.S.	126	127
Germany	8	38
Israel	1	37
Netherlands	32	33
Singapore	17	17
Hong Kong	8	10
U.K.	7	7
Japan	2	3
Australia	3	3

Sweden	1	2
Mexico	2	2
Italy		2
India	1	2
Indonesia	1	2
France	2	2
U.A.E.	2	2
Poland		1
Norway	1	1
Kenya	1	1
Iraq	1	1
Ireland	1	1
Hungary		1
Cyprus	1	1
Colombia	1	1
Brazil		1
Total	**219**	**298**

Table 7: Servers potentially associated with Cobwebs product deployments and its wider server infrastructure.

When considering all hosts including those we cannot attribute to product deployments, we identified 298 servers associated with Cobwebs server infrastructure located in 25 countries. This includes all currently resolving cobwebsapp.com, cwtapp.com, and cwsystem.com subdomains and the additional hosts identified via Censys. According to this analysis, we identified servers in additional countries (Brazil, Italy, Poland, Hungary) and a much higher number of servers located in Israel (37). Notably, 71 servers are located in the Netherlands and Germany. Most of the U.S. servers are located in the state of Virginia, followed by Washington, California, Arizona, Texas, Illinois, and Oregon.

According to an analysis of IP addresses, 219 out of the 298 active hosts affiliated with Cobwebs Technologies' server infrastructure are hosted in data centres related to Microsoft's Azure cloud.

Some host names associated with Cobwebs product servers have been resolving to the same IP address for only a few months. Many have been active for several years. IP addresses of product servers that have been active only in the past are currently located in additional countries (Switzerland, Portugal, and Lithuania).

While we have high confidence in the list of countries where we identified active servers associated with Cobwebs products, we know neither whether these products are actually in operation, nor whether the customers who are potentially using Tangles and other Cobwebs products are located in the same countries as the located servers. We do not consider our map of Cobwebs product servers to be exhaustive. While we identified 219 potential product servers, the numbering in the subdomain names ranges from low digits up to 1704.

Potential Webloc Servers

Based on the above research, we identified five subdomains that contain the letters ‘wl’ in the host name, which may refer to the Webloc product:

Host name	Resolving to IP	First seen	Last seen	Latest server location
wl-s374.cobwebsapp.com	81.182.253.140	2022-02-10	2026-01-17	Hungary
s637-wl.cobwebsapp.com	201.163.8.204 189.254.151.40	2023-03-29 2022-06-29	2026-03-14 2023-03-29	Mexico
s704-wl.cobwebsapp.com	13.81.242.125	2023-04-25	2026-03-14	Netherlands
wl-angel6.cobwebsapp.com	168.63.232.11	2022-07-27	2026-03-14	Singapore
wl-azdep06.cobwebsapp.com	40.127.96.53		2020-12-07	Ireland

Table 8: Potential Webloc servers

The locations of currently active servers associated with potential Webloc deployments include Mexico (from 2022), Singapore (from 2022), and the Netherlands (from 2023). A server associated with a potential Webloc deployment in Hungary was active from 2022, but stopped being active in January 2026. Another potential Webloc server active in 2020 resolves to an IP address that is currently located in Ireland.

We have medium confidence in the assessment that host names containing the letters ‘wl’ represent Webloc servers. Based on our findings about Webloc customers we do not believe that this list is comprehensive in any way.

7. Links to Quadream and Other Spytech Vendors

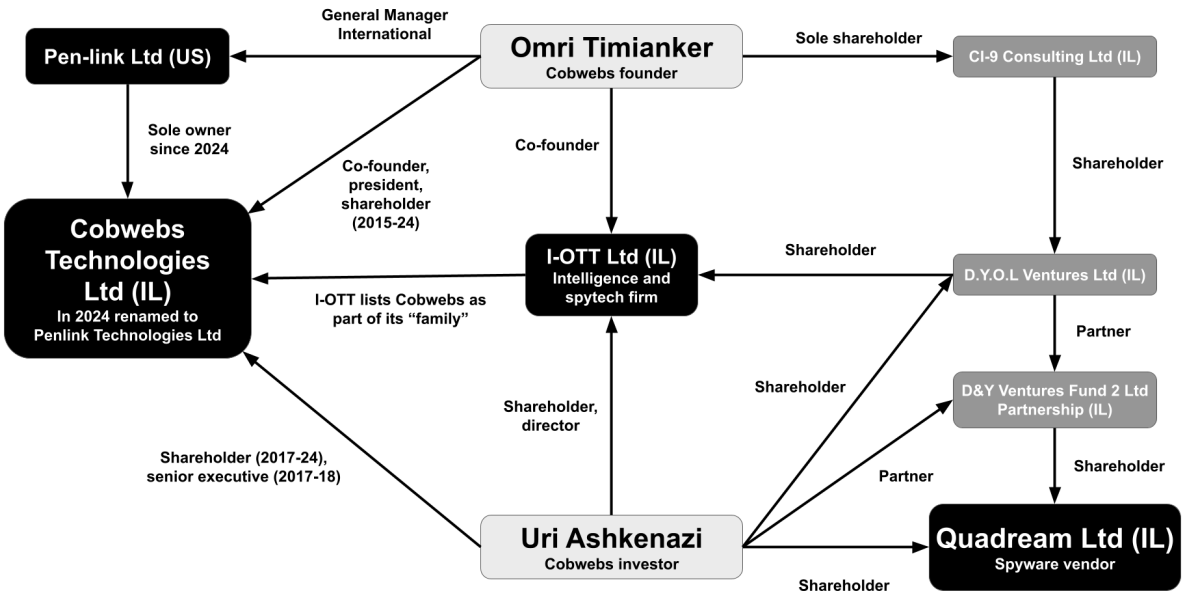


Figure 14: Cobwebs corporate network

Cobwebs Technologies has links to the spyware vendor Quadream through Cobweb Technologies' founder Omri Timianker and investor Uri Ashkenazi. The Citizen Lab previously revealed that Quadream's spyware was used to target civil society in North America, Central Asia, Southeast Asia, Europe, and the Middle East. Victims included journalists and political opposition figures. While it was reported that Quadream was trying to sell its assets in 2023, it is unclear whether it has managed to do so, and, according to company registration documents, Quadream continues to operate as an entity in Israel. According to company registration documents from Israel, both Timianker and Ashkenazi are also affiliated with a company called I-OTT, an intelligence and surveillance technology firm that has advertised providing "combat training" for "guerrilla warfare" and consultations on "covert operations."

Cobwebs Founder: Omri Timianker

Omri Timianker is the founder of Cobwebs Technologies Ltd. and now oversees Penlink's international operations.[51] According to documents obtained from Israel's company register, he also has an indirect interest in Quadream Ltd. **Figure 14** contains information obtained from the Israel's company register and reveals the ownership chain that links Timianker with Quadream.

[51] https://www.linkedin.com/in/omri-timianker/details/experience/, accessed 1.3.2026

Timianker's LinkedIn profile[52] claims that as co-founder and president of Cobwebs (2015-2024), his key achievements included "scaling global operations across government and commercial markets" and "driving hundreds of large-scale deployments in complex environments." According to his LinkedIn, he is now "General Manager International" at Penlink and responsible for leading "global growth and market expansion for Penlink across all regions outside the Americas."

In 2025, Timianker co-founded insAIghts Academy, a digital intelligence "academy" with training hubs in Israel, London and the U.S.[53] A promotional video on YouTube for the training centre in London states that the "purpose of insAIghts is to train the intelligence officers of the future." InsAIghts offers training on "deep data extraction"
enabling participants to "gain the ability to uncover essential, hidden information." InsAIghts offers their training not only to law enforcement but also to those who work in finance or the "corporate world."

According to the firm's website, Timianker is also on the advisory board of Titan Ventures, a venture capital firm that invests in Israel's cyber-intelligence sector. It claims that it has gained "deep market understanding and expertise through years of involvement," and is able to "identify the lack of adequate intelligence solutions to cope with the current technological and operational challenges." According to his LinkedIn profile, Timianker also co-founded I-OTT (2011-2021). Timianker, according to his bio on the Titan Ventures website, also founded I-OTT (see below).

Uri Ashkenazi

As previously reported by the Citizen Lab, Uri Ashkenazi is an Israeli financier who invests in Israel's cyber intelligence sector, primarily through his venture capital firm, Titan Ventures. Ashkenazi has been a key investor in Quadream, Cobwebs, Falkor, and I-OTT. *Intelligence Online* reported that he also previously served as a senior vice president of finance at Cobwebs. According to his LinkedIn profile he served in this role from January 2017 to October 2018.

Ashkenazi is closely connected to Omri Timianker. When Timianker posted news of the Penlink partnership on LinkedIn, Ashkenazi responded that it had been an "honor and privilege to invest, partner and support you guys from the early days." To which Timianker replied "Thanks Ori Ashkenazi my Trustable friend, lets continue to rock and roll together."[54] In addition to the pair being connected through Cobwebs, Ashkenazi and Timianker are linked through I-OTT, Titan Ventures, and D&Y Ventures; Ashkenazi is the managing partner of Titan Ventures[55] and according to Israel corporate records, also a shareholder in D&Y Ventures and a shareholder in I-OTT.

---

[52] https://www.linkedin.com/in/omri-timianker-2a41925/, accessed 1.3.2026
[53] https://www.linkedin.com/in/omri-timianker-2a41925/, accessed 1.3.2026
[54] https://www.linkedin.com/posts/omri-timianker-2a41925_cobwebs-digitalabrintelligence-activity-7084554769092026368-Fg4r/, accessed 1.3.2026
[55]

I-OTT

On its website, I-OTT advertises itself as “customized intelligence solutions for governmental and private agencies” and claims to have offices in Israel, Mexico and Brazil. According to the website, Cobwebs and Titan Ventures are part of the I-OTT “family."

The 2017 version of its website reveals I-OTT product capabilities claiming that their “analysts have a rich military and civilian intelligence background, powerful automated WEBINT systems and the support of virtual persona (sock puppet),” and that they could provide “targeted research reports concerning almost any topic” including “social unrest." They also claim to be operating “tailor-made avatars for collecting sensitive information." In addition to their technology offering, I-OTT offered “advanced combat training” and claimed to "provide the basic effective ‘toolbox’ for anti-terror and guerrilla warfare,” along with “training and consulting about covert operations and units."

According to Intelligence Online, the company Falkor is a spin off of I-OTT and specializes in mass data analysis. Falkor’s website urges its customers through the use of their products to “connect to OSINT and SOCMINT sources and enrich your data with new identifiers, associated online accounts, posts, and more. Conduct digital profiling and monitor topics of interest in real-time."

8. Trapdoor

We present additional research on Trapdoor, a product developed by Cobwebs Technologies that has rarely been discussed publicly. In a 2020 article, the trade press site *Intelligence Online* reported that Trapdoor is a Cobwebs solution “reserved for government customers.”

Cobwebs Website

The 2021 website of Cobwebs Technologies promoted Trapdoor as a system for “active web intelligence” that allows customers to “[a]nonymously engage with threat actors with various communication methods” and “re-build any link from across the web” in order to “gather intelligence” from devices including IP addresses, device type, “cookies," and language settings. Trapdoor would facilitate the “remote extraction of technical details with non-intrusive methods,” but also provides “methods to launch directed command modules at a connected source." These promotional phrases are rather hard to parse.

Trapdoor Specifications

A Vietnamese “Technical Specifications” document[56] dated 2021 and branded “Cobwebs Technologies” we discovered publicly available on the web contains a clearer description of Trapdoor capabilities. The

[56] Accessed on 12.3.2026 and archived by the authors: https://www.studocu.vn/vn/document/hoc-vien-cong-nghe-buu-chinh-vien-thong/ki-thuat-lap-trinh/7-webint-specifications/118733920, accessed 12.3.2026

document appears to provide contractual requirements for the deployment of a “WEBINT” system including the Cobwebs products Tangles, Lynx, Trapdoor, and Webloc. The requirements listed in the document are very specific, overlapping with product descriptions from other sources in several ways.

While the document is largely in Vietnamese, the Trapdoor requirements section refers to the system as “SEP/Trapdoor” in English. The Vietnamese term used in the section translates to “social engineering platform." We conclude that the document describes Trapdoor as a “social engineering platform," in short “SEP."

The Trapdoor section describes requirements the system must meet and thus makes suggestions about the system’s capabilities. As translated by the authors of this report with the help of machine translation tools, it states that:

- Trapdoor is a “web-based social engineering module to actively interact with targets," separate from the “passive intelligence systems” for “web intelligence” and “avatar management” from the same vendor.
- The system provides the ability to “generate phishing links disguised as any web link that can be sent to targets” via email or SMS. It supports “link obfuscation” using “URL shorteners," supporting the “redirection of visitors to specified websites without exposing server details." It allows “analysts to apply social engineering techniques such as sending pop-ups, pages, and input requests” to collect information.
- It includes tools to “rapidly design full web pages or pop-ups deployed on the target side," supporting “styling, content editing, image modification, input requests, file attachments, mobile and desktop compatibility." It supports “URLs across multiple domains” that can be “registered anonymously, with flexibility for the end user to choose domain names."
- It maintains a “list of all links or websites accessed through the system." It “route[s] and “host[s] target connections through proxy infrastructure and ensure anonymity and non-traceability," provides a “dashboard” showing “real-time and historical connection data” and triggers “alerts” upon “target connection."
- It “automatically extract[s] available information from target connections” including IP address, browser type, language, version and plugins, operating system and version, device type, CPU and GPU information, screen resolution, ISP information, estimated geolocation, user inputs, timezone, battery level and charging status. If available it also provides “social media details” and “location network details."
- The system includes a “keylogger to record keystrokes, including potential capture of usernames and passwords."
- In addition, it allows “analysts to perform actions on the target’s browser, including terminating active connections, opening hidden tabs, extracting media from the target device, sending pop-ups, and delivering files or payloads."

Trapdoor Source Code

We discovered servers that display Trapdoor login pages, as of March 2026. When accessing one of these pages in the web browser, it loaded Javascript code related to Trapdoor. Based on our analysis, we assess that the code represents a version of the Javascript source code of the Trapdoor admin interface used by customers to operate the system.

The source code refers to a Trapdoor "clientapp" as part of a Cobwebs software release version 5.

```
C:/Code/Cobwebs/Cobwebs_Release_V5/cobwebs/Trapdoor/clientapp
```

We refer to this "client application" as the Trapdoor admin interface. The source code suggests that Trapdoor provides tools to add and manage email messages, SMS messages, short URLs, domains for web pages, and domains for email delivery (**Table 9**, left column):

Trapdoor user interface tools Code labels: toolsPagesModule, top-bars.tools.pages	**Trapdoor activity types** Code labels: activity-page.html, TrapdoorActivityType	**Trapdoor event types** Code labels: components/events-grid, EventTypes
toolsMainPage shortenersMainPage shortenersAddPopup shortenersGrid domainsMainPage domainsAddPopup domainsGrid emailDomainsMainPage emailDomainsAddPopup emailDomainsGrid smsMainPage smsAddPopup smsGrid mailsMainPage mailsAddPopup mailsGrid proxyMainPage proxyAddPopup proxyGrid	Microphone Media GetPopup Location PayLoads FakePage FingerPrints GetLocalIp IdentifyProxy SocialNetworks Tor LocalNetworks PortScan HardwareInfo SmsSent EmailSent SendKeyboradData [sic] TerminateConnection OpenAdditionalTab	Location Credentials Microphone Camera Fingerprints ProxyIdentified NewIpFound ActionStarted ErrorCaught ResponsiveIps OpenPorts DeviceType Tor LoggedInNetworks HardwareInfo ScreenshotTaken SensorsData TimeZone

Table 9: Excerpts from the Javascript source code of the Trapdoor "clientapp."

According to the source code, Trapdoor also allows customers to perform different "activities" related to the creation of fake websites, opening additional browser tabs, sending keyboard data and the delivery of emails, SMS, and "PayLoads" (**Table 9**, centre column). Other activities carried out by the system, which are referred to as "events," involve device fingerprints, sensor data, "credentials" and "microphone," "camera" (**Table 9**, right column). The code labels in the table headers describe and

contextualize the three lists of terms presented in the table. While a comprehensive analysis of the source code is beyond the scope of this report, the list of tools, activity types and event types in the code corroborates the capabilities described in the technical specifications document, as we discuss next.

Analysis and Assessment of Trapdoor Capabilities

The descriptions of Trapdoor capabilities on the 2021 Cobwebs website and in the Vietnamese "Technical Specifications" document, in combination with the source code analysis, suggest that Trapdoor helps customers to trick victims into revealing information by sending them phishing links that lead to fake web pages, which are also created with the help of Trapdoor.

When a victim accesses those fake web pages, the system provides the Trapdoor customer with information entered by the victim, which can include keystrokes, usernames and passwords, and with information on the victim's device. Most device attributes that can be extracted from "target connections" according to the Vietnamese document, are clearly accessible to website operators without compromising the victim's device, including IP, device and browser information. Battery level and charging status of a device have also been accessible to parties who serve web pages to someone's browser.

In addition, our analysis suggests that Trapdoor customers can remotely carry out offensive actions that affect the victim's browser or device. This includes opening pop-up windows and hidden tabs in the victim's web browser and even "delivering files or payloads" to the victim's device. According to the commonly used definition in the cybersecurity context, the term "payload" typically refers to malicious software downloaded to a device. Based on our analysis, we assess that Trapdoor can help facilitate the deployment of malware on a victim's device but does not include remote device infection or malware capabilities itself.

Our analysis of the technical specifications and the source code also leads us to conclude that Trapdoor can likely provide at least some capabilities typically provided by malware compromising a device's operating system, including access to "media from the target device,"[57] camera and microphone. As the system focuses on the extraction of information based on web pages visited by the victim, we assume that access to camera and microphone is or was also based on code executed in the victim's web browser.

As discussed above, Cobwebs Technologies' 2021 website referred to Trapdoor as a system for "active web intelligence" that facilitates "remote extraction of technical details with non-intrusive methods" but also provides "methods to launch directed command modules at a connected source."

[57] According to the Trapdoor requirements section in the "Technical Specifications" document described above, as translated by the authors of this report with the help of machine translation tools.

Our findings on Trapdoor capabilities align with the findings in the "Threat Report on the Surveillance-for-Hire Industry" published by Meta in 2021, which observed that "accounts used by Cobwebs customers also engaged in social engineering to join closed communities and forums and trick people into revealing personal information." While Cobwebs Technologies stated that the report was "false," the research laid out in this section suggests that Meta had observed an application of Trapdoor's capabilities in the wild.

Trapdoor Customers

We could not identify any Trapdoor customers and we do not know whether the system is still being sold by Penlink. Trapdoor is not promoted on Penlink's website. However, we identified servers active in 2026 that display Trapdoor login pages in the browser, one of them loading Javascript code related to the system's admin interface, as discussed above.

Potential Trapdoor Servers

We identified two currently active servers located in Kenya and Indonesia that displayed login pages including a Trapdoor logo when accessing them in the web browser, based on searching for hosts associated with Trapdoor using Censys:

IP address	Port	Server location	Trapdoor login page observed
41.215.20.45	3701	Kenya	2026-03-14
139.0.5.194	1300	Indonesia	2026-03-14

Table 10: Potential Trapdoor servers

Based on our mapping of Cobwebs server infrastructure, we identified four currently active servers located in Japan, United Arab Emirates, Singapore and Hong Kong that contain the letters 'td' in the host name, and thus may be associated with additional Trapdoor deployments:

Host name	Resolving to IP	First seen	Last seen	Latest server location
s470-td.cobwebsapp.com	104.41.161.13	2024-01-03	2026-03-14	Japan
s883-td.cwsystem.com	20.74.133.244	2023-01-03	2026-03-14	UAE
td-al.cobwebsapp.com	13.76.212.122	2024-01-06	2026-03-14	Singapore
td-rtn.cobwebsapp.com	207.46.155.220	2020-08-08	2026-03-14	Hong Kong

Table 11: Potential Trapdoor servers

As discussed in **Section 6**, we have medium confidence in the assessment that host names containing the letters 'td' represent Trapdoor servers. Three additional servers containing the letters 'td' in the host name that were active until 2025 resolve to IP addresses currently located in Singapore, Israel, and Germany:

Host name	Resolving to IP	First seen	Last seen	Latest server location
td-s315.cobwebsapp.com	20.52.38.61	2024-01-17	2025-08-05	Germany
s464-td.cobwebsapp.com	147.234.85.11	2023-03-02	2025-08-07	Israel
s490-td.cobwebsapp.com	20.205.226.167	2022-03-10	2025-08-07	Singapore

Table 12: Potential historical Trapdoor servers

In conclusion, we identified potential Trapdoor deployments located in Kenya and Indonesia based on observing Trapdoor login pages in the web browser. We identified four potential Trapdoor deployments located in Japan, United Arab Emirates, Singapore, and Hong Kong based on the assessment that host names affiliated with Cobwebs Technologies that contain the letters 'td' may represent Trapdoor servers.

9. Responses

On April 3, 2026, we sent a summary of our findings to Penlink and offered them the opportunity to reply, which we publish here in full.

Penlink claims in its response to the Citizen Lab that our findings "appear to rely on either inaccurate information or a misunderstanding about how we operate, including practices that Penlink does not engage in following our acquisition of Cobwebs Technologies in 2023." It states that we "identify companies and products that no longer exist," as well as "list countries we do not do business in" or "describe products incorrectly," without being specific about the companies, products and countries. The response further states that "Penlink complies with U.S. state privacy laws" and that "Penlink understands the sensitivity and complexity of data privacy and operates under thoughtful compliance, due diligence, and responsible-use standards."

We address some issues raised by Penlink in several places throughout the report. Its response leaves many of the questions we sent to them unanswered, adding to the lack of information it publicly provides about Webloc, its capabilities, customers, and uses. The response also does not address compliance with privacy and data protection laws outside the U.S., including in Europe.

10. Conclusion

Both Cobwebs Technologies, which developed Webloc, and its successor Penlink, which has been selling Webloc since 2023, do not provide much public information about the system and its customers. This report provides a first comprehensive mapping of the capabilities, data processing practices, and customers of Webloc, a mass surveillance system that relies on data purchased from everyday consumer apps and digital advertising that provides information on the whereabouts, movements and personal characteristics of entire populations.

Intrusive Mass Surveillance

Webloc covertly monitors hundreds of millions of people globally based on commercial data obtained from smartphones and other mobile devices they use. Even if a customer uses Webloc to track only a few individuals, the system still processes a constantly updated data stream on a large number of people without probable cause.

Location data and similar data collected from apps and digital advertising are highly sensitive. They can reveal information about a person's home, workplace, family, friends, religion, political views, sexual orientation or health issues. As such, we consider Webloc to be an intrusive mass surveillance system.

Disproportionate Surveillance

In his book on the origins of ad-based surveillance in the U.S., investigative journalist Byron Tau shows how these technologies, initially built for U.S. military and intelligence operations in war zones, were eventually also deployed domestically by federal law enforcement agencies and then trickled down to state and local police. A local police department in the U.S., which purchased Webloc for border security and sex trafficking investigations, explained that it soon discovered other applications of the technology and began to use the system for routine criminal cases with damages of a few thousand dollars, according to an internal report discussed in **Section 4**. This type of mission creep is particularly concerning because of the disproportionate nature of ad-based surveillance systems and because our findings show such systems are now used by military, intelligence and law enforcement agencies, including local police units, in several countries around the globe.

Legally Questionable

The systematic misuse of data purchased from everyday consumer apps and digital advertising for warrantless surveillance raises serious concerns about civil liberties and fundamental rights, particularly when used to target vulnerable groups such as immigrants or those who exercise their freedom of expression and assembly rights. Ad-based surveillance raises specific concerns when applied by organizations or governments, which are prone to authoritarianism or have weak or limited oversight. It generally raises concerns when governments lack a lawful basis to use it or when the underlying data is processed without a lawful basis.

In the U.S. and in Europe, both the lawfulness of governments using ad-based data for surveillance and the lawfulness of sharing the data over the entire supply chain, from apps and advertising firms to data brokers and surveillance vendors, are highly controversial.

In recent cases against several data brokers in the U.S., the Federal Trade Commission (FTC) made clear that their location data sales were unfair business practices in violation of federal law. Scholars, lawmakers and many civil society organizations have considered the use of commercial data purchased from consumer data brokers and advertising firms for surveillance conducted by government agencies as a circumvention of the Fourth Amendment. In 2023, the DHS itself found in a report that its agencies violated federal law through their use of purchased location data, stating that ICE, CBP, and the Secret Service did not adhere to existing internal privacy policies and did not have sufficient policies and procedures in place.

In Europe and the U.K., the lawfulness of using the data is controversial even for targeted advertising purposes. Consumer apps and digital advertising firms selling data to governments for surveillance purposes, and thus for entirely different purposes than what was stated to consumers, violates the principle of purpose limitation, a cornerstone of the European data protection regime. While the use of the data by governments for public safety and national security is subject to separate and different national legislation, its lawfulness is questionable and it lacks adequate oversight in several European countries.

Legal Justifications

We are not aware of public statements that clearly explain how Penlink, and previously Cobwebs Technologies, obtain the data specifically used in the Webloc product in compliance with privacy and data protection legislation. As discussed in **Section 3**, two documents that describe Webloc, dated 2021, claim that data collection complies with the GDPR and "various" privacy laws and emphasize that the data is collected with the "consent" of those who are monitored by the system. A promotional brochure from 2020 stated that Webloc provides the capability to "find anonymous threat actors." The LAPD stated that it uses "commercially available anonymized data," when asked about Webloc.

Both the claims that data from mobile apps and digital advertising were "anonymized" and sold based on "consent" represent the two main legal justifications used across the consumer data industry and also by ad-based surveillance vendors.

In Europe, under the GDPR, location records and behavioral data linked to Advertising IDs or other personal identifiers are not anonymous but personal data. The high standard that the GDPR sets for "informed" consent makes it unlikely that any actor in the supply chain, from mobile app vendors and advertising firms to ad-based surveillance vendors, can rely on valid consent for sharing data collected for the purpose of operating apps or digital advertising for surveillance purposes.

In the U.S., the FTC recently clarified that Advertising IDs “offer no anonymity in the marketplace," because “many” businesses “regularly link” those IDs “to other information about them, such as names, addresses, and phone numbers." In a case against a data broker which relied on the “consent” of those whose location data was collected and sold to government agencies, the FTC determined that consumers did not actually consent.

Even if location records would not include personal identifiers, such as an Advertising ID, they are not truly anonymous and can be re-identified, as academic research has often shown. As discussed in **Section 3**, identifying persons who use the tracked devices is, in fact, one of the purposes of Webloc.

Penlink recently claimed that Webloc’s data providers “filter out sensitive locations, such as hospitals, schools, and religious institutions," reflecting one of several orders the FTC recently imposed on location data brokers. We do not know whether this claim is defensible. If it was, it addresses only one of several legal issues underlying Webloc's data processing.

Penlink provides a generic privacy policy on its website, which does not mention Webloc and covers everything from data processing on visitors of penlink.com to the collection of information from third-party sources and its disclosure to customers of Penlink’s “intelligence and analytics platforms”. It emphasizes that Penlink and its affiliates “value your privacy.” It explains that Penlink may receive data on individuals from “data brokers” and “other commercially available sources,” including name, email, phone number, and “historical information about the precise geolocation of your device,” and that it may disclose the information it collects with its customers. The policy also lists a number of “rights” people “may have” in the E.U., U.K., and several U.S. states, and links to a page where people can “opt out of sales of personal information to customers.” Penlink is registered as a “data broker” in the California Data Broker Registry.

Recommendations for States and Regulatory Bodies

- In Europe and the U.K., national data protection authorities are responsible for enforcing the GDPR, and in all but two E.U. member states also for enforcing the Law Enforcement Directive (LED), which regulates personal data processing for law enforcement purposes. These authorities need to proactively investigate potential violations of the rights and freedoms of European data subjects due to the operation of Webloc and all entities involved in Webloc’s data supply chain.
- Our findings suggest that European governments are particularly nontransparent about their potential use of ad-based surveillance technologies citing public safety and national security reasons. The public interest in a democratic debate about these technologies must be given higher priority than keeping information confidential for security reasons, specifically when it comes to law enforcement, and especially because the systems we examined enable highly intrusive mass surveillance.
- Governments in Europe, U.K., U.S., and other regions must ensure that intrusive surveillance based on commercial data purchased from mobile apps, advertising firms and consumer data

brokers does not infringe on civil liberties and fundamental rights by implementing adequate safeguards and democratic oversight.
- Ad-based surveillance relies on the way mobile apps and digital advertising currently operate, leading to uncontrolled data sharing with a large number of third parties. This broken digital infrastructure needs to be reformed at several levels, as consumer associations, regulators and policymakers have long been demanding.
- The urgent need to reform data practices in digital advertising and in the mobile app ecosystem is further aggravated by concerns about the broad availability of highly sensitive data on defense personnel and political leaders, which has been deemed a security risk by civil society organizations and U.S. intelligence agencies alike.
- It is imperative that governments exercise rigorous due diligence regarding vendors when procuring surveillance technologies, including Webloc, Tangles, and other products. The assessment should include a detailed analysis of capabilities and data processing activities over the entire data supply chain in relation to legal requirements, potential abuses of the product, and the vendor's broader business practices.

Further Research

Based on our findings, we believe that further research would be fruitful with respect to:

- additional potential Webloc customers in Europe, in the U.K., U.S. and other regions where we received inconsistent or unsatisfactory responses to freedom of information requests, or found other indications for potential Webloc sales or usage,
- Webloc's data sources and data supply chain, i.e. app vendors, digital advertising firms or data brokers which the system obtains data from,
- how Webloc is being used by law enforcement agencies and other customers and how this affects persons who are being tracked and profiled with the help of the system,
- cases of mission creep, in which Webloc's highly intrusive technology is used to investigate petty crimes, or cases falling outside of the appropriate scope of an agency's mandate.

This report is part of an ongoing series of investigations we are doing on the use of commercial data for surveillance purposes. We will be publishing subsequent investigations that explore areas for further research we have flagged in this report.

Protect Yourself from Ad-Based Surveillance

Ad-based surveillance relies on data sent from the apps installed on your mobile device to third parties. Any app that displays advertisements is potentially affected. Apps that do not display ads may also directly or indirectly share user data with third parties. To minimize how apps installed on your device share data with third parties you can take the following steps:

- Apple iOS devices offer some protection against apps sharing data with third parties. When installing a new app, deny it the permission to "track your activity across other companies' apps and websites" during installation. Review the apps you have previously granted the permission to track you. This functionality is not available on Apple devices with an iOS version older than 14.5. In addition, review the apps you may have granted the permission to access your location and other information from your device.
- For Android devices, the "advertising ID" assigned to your device is key to any tracking and profiling carried out by third parties. Depending on the device vendor and Android version, delete the advertising ID or opt out of ads personalization in the settings. In addition, review the apps you may have granted the permission to access your location and other information from your device.

More information is available on the websites of the California Privacy Protection Agency, Canadian Centre for Cyber Security, Privacy International and EFF.

Following these recommendations, you can minimize but not reliably prevent apps from sharing data with third parties. A mobile app may still share data it processes for the purpose of operating the app on its servers directly with other companies. Google itself states that apps might use other "persistent or proprietary identifiers" when a user deletes the advertising ID on their device. App vendors and third parties constantly try to find ways around existing protections.

Appendix

Subdomains Related to Potential Cobwebs Product Servers

List of 215 host names that we consider to be affiliated with Cobwebs products deployments, resolving to particular IP addresses as of January 30, 2026. 106 hosts, marked with an asterisk, displayed a login page related to a Cobwebs product in the browser, as of March 6, 2026.

```
s12-tg[.]cobwebsapp[.]com
tg-poc62[.]cobwebsapp[.]com
tg-101[.]cobwebsapp[.]com
tg-102[.]cobwebsapp[.]com
tg-103[.]cobwebsapp[.]com
tg-107[.]cobwebsapp[.]com
tg-118[.]cobwebsapp[.]com
tg-119[.]cobwebsapp[.]com
tg-151[.]cobwebsapp[.]com
tg-157[.]cobwebsapp[.]com
tg-173[.]cobwebsapp[.]com
tg-180[.]cobwebsapp[.]com
tg-s313[.]cobwebsapp[.]com
tg-s329[.]cobwebsapp[.]com
tg-s356[.]cobwebsapp[.]com
```

wr-s361[.]cobwebsapp[.]com
s446-tg[.]cobwebsapp[.]com
s452-tg[.]cobwebsapp[.]com
s457-tg[.]cobwebsapp[.]com
s470-td[.]cobwebsapp[.]com
s472-tg[.]cobwebsapp[.]com
s479-tg[.]cobwebsapp[.]com
s484-tg[.]cobwebsapp[.]com
s534-tg[.]cobwebsapp[.]com
s558-tg[.]cobwebsapp[.]com
s562-tg[.]cobwebsapp[.]com
s578-tg[.]cobwebsapp[.]com
s629-tg[.]cobwebsapp[.]com
s635-tg[.]cobwebsapp[.]com
s637-wl[.]cobwebsapp[.]com
s639-tg[.]cobwebsapp[.]com
s640-tg[.]cobwebsapp[.]com
s641-tg[.]cobwebsapp[.]com
s654-tg[.]cobwebsapp[.]com
s655-tg[.]cobwebsapp[.]com
s657-tg[.]cobwebsapp[.]com
s658-tg[.]cobwebsapp[.]com
s659-tg[.]cobwebsapp[.]com
s669-tg[.]cobwebsapp[.]com
s670-tg[.]cobwebsapp[.]com
s671-tg[.]cobwebsapp[.]com
s673-tg[.]cobwebsapp[.]com
s683-tg[.]cobwebsapp[.]com
s689-tg[.]cobwebsapp[.]com
s698-tg[.]cobwebsapp[.]com
s703-tg[.]cobwebsapp[.]com
s704-wl[.]cobwebsapp[.]com
s706-tg[.]cobwebsapp[.]com
tg-sys1228[.]cobwebsapp[.]com
tg-zu1[.]cobwebsapp[.]com
tg-sh[.]cobwebsapp[.]com
tg-cmp[.]cobwebsapp[.]com
wr-fiam[.]cobwebsapp[.]com
tg-kbq[.]cobwebsapp[.]com
tg-rtn[.]cobwebsapp[.]com
td-rtn[.]cobwebsapp[.]com
tg-tony01[.]cobwebsapp[.]com
tg-sgm[.]cobwebsapp[.]com
wl-angel6[.]cobwebsapp[.]com
tg-ang[.]cobwebsapp[.]com
td-al[.]cobwebsapp[.]com
tg-xl-6[.]cobwebsapp[.]com
tg-ospa[.]cobwebsapp[.]com

tg-bcpd[.]cobwebsapp[.]com
tg-nine[.]cobwebsapp[.]com
tg-bcpo[.]cobwebsapp[.]com
p01-tg[.]cwsystem[.]com (*)
p02-tg[.]cwsystem[.]com (*)
p03-tg[.]cwsystem[.]com (*)
p03-um[.]cwsystem[.]com
p06-tg[.]cwsystem[.]com
p07[.]cwsystem[.]com (*)
p09-tg[.]cwsystem[.]com
p11-tg[.]cwsystem[.]com
p12-tg[.]cwsystem[.]com
p30-tg[.]cwsystem[.]com
p31-tg[.]cwsystem[.]com (*)
p51-tg[.]cwsystem[.]com (*)
p52-tg[.]cwsystem[.]com
p53-tg[.]cwsystem[.]com
p56-tg[.]cwsystem[.]com
p57-tg[.]cwsystem[.]com (*)
p58-tg[.]cwsystem[.]com (*)
p062-tg[.]cwsystem[.]com
p70-tg[.]cwsystem[.]com
p73-tg[.]cwsystem[.]com (*)
p81-tg[.]cwsystem[.]com (*)
p82-tg[.]cwsystem[.]com
p83-tg[.]cwsystem[.]com (*)
p86-tg[.]cwsystem[.]com
p87-tg[.]cwsystem[.]com (*)
p92-tg[.]cwsystem[.]com
p93-tg[.]cwsystem[.]com (*)
p100-tg[.]cwsystem[.]com (*)
p101[.]cwsystem[.]com (*)
p102-tg[.]cwsystem[.]com
p107-tg[.]cwsystem[.]com
p110-tg[.]cwsystem[.]com (*)
p111[.]cwsystem[.]com (*)
p122-tg[.]cwsystem[.]com (*)
p141[.]cwsystem[.]com
p148[.]cwsystem[.]com
p154[.]cwsystem[.]com (*)
p156[.]cwsystem[.]com (*)
p159[.]cwsystem[.]com
p160[.]cwsystem[.]com (*)
p161[.]cwsystem[.]com
p167[.]cwsystem[.]com (*)
p172[.]cwsystem[.]com
p177[.]cwsystem[.]com
p178[.]cwsystem[.]com (*)

p184[.]cwsystem[.]com (*)
p188[.]cwsystem[.]com (*)
p189[.]cwsystem[.]com
p200-tg[.]cwsystem[.]com
s883-td[.]cwsystem[.]com
s41-tg[.]cwtapp[.]com (*)
s115-tg[.]cwtapp[.]com (*)
s255-tg[.]cwtapp[.]com (*)
s285-tg[.]cwtapp[.]com (*)
s521-tg[.]cwtapp[.]com (*)
s702-tg[.]cwtapp[.]com
s712-tg[.]cwtapp[.]com
s713-tg[.]cwtapp[.]com (*)
s733-tg[.]cwtapp[.]com (*)
s734-tg[.]cwtapp[.]com
s740-tg[.]cwtapp[.]com (*)
s741-tg[.]cwtapp[.]com (*)
s742-tg[.]cwtapp[.]com
s753-tg[.]cwtapp[.]com (*)
s765-tg[.]cwtapp[.]com (*)
s790-tg[.]cwtapp[.]com
s808-tg[.]cwtapp[.]com (*)
s843-tg[.]cwtapp[.]com
s851-tg[.]cwtapp[.]com
s863-tg[.]cwtapp[.]com
s865-tg[.]cwtapp[.]com (*)
s866-tg[.]cwtapp[.]com (*)
s874-tg[.]cwtapp[.]com (*)
s877-tg[.]cwtapp[.]com (*)
s880-tg[.]cwtapp[.]com (*)
s882-tg[.]cwtapp[.]com (*)
s884-tg[.]cwtapp[.]com (*)
s892-tg[.]cwtapp[.]com
s896-tg[.]cwtapp[.]com
s940-tg[.]cwtapp[.]com (*)
s950-tg[.]cwtapp[.]com (*)
s973-tg[.]cwtapp[.]com (*)
s974-tg[.]cwtapp[.]com (*)
s992-tg[.]cwtapp[.]com
s1008-tg[.]cwtapp[.]com
s1012-tg[.]cwtapp[.]com (*)
s1019-tg[.]cwtapp[.]com (*)
s1026-tg[.]cwtapp[.]com (*)
s1038-tg[.]cwtapp[.]com (*)
s1040-tg[.]cwtapp[.]com (*)
s1042-tg[.]cwtapp[.]com (*)
s1058-tg[.]cwtapp[.]com (*)
s1060-tg[.]cwtapp[.]com (*)

s1069-tg[.]cwtapp[.]com (*)
s1084-tg[.]cwtapp[.]com (*)
s1087-tg[.]cwtapp[.]com (*)
s1093-tg[.]cwtapp[.]com (*)
s1097-tg[.]cwtapp[.]com (*)
s1111-tg[.]cwtapp[.]com (*)
s1113-tg[.]cwtapp[.]com (*)
s1121-tg[.]cwtapp[.]com (*)
s1123-tg[.]cwtapp[.]com (*)
s1129-tg[.]cwtapp[.]com (*)
s1143-tg[.]cwtapp[.]com (*)
s1146-tg[.]cwtapp[.]com
s1150-tg[.]cwtapp[.]com (*)
s1152-tg[.]cwtapp[.]com (*)
s1169-tg[.]cwtapp[.]com (*)
s1177-tg[.]cwtapp[.]com (*)
s1201-tg[.]cwtapp[.]com (*)
s1210-tg[.]cwtapp[.]com (*)
s1212-tg[.]cwtapp[.]com (*)
s1213-tg[.]cwtapp[.]com (*)
s1219-tg[.]cwtapp[.]com (*)
s1221-tg[.]cwtapp[.]com (*)
s1232-tg[.]cwtapp[.]com (*)
s1249-tg[.]cwtapp[.]com (*)
s1254-tg[.]cwtapp[.]com (*)
s1258-tg[.]cwtapp[.]com (*)
s1260-tg[.]cwtapp[.]com (*)
s1268-tg[.]cwtapp[.]com
s1275-tg[.]cwtapp[.]com (*)
s1297-tg[.]cwtapp[.]com (*)
s1300-tg[.]cwtapp[.]com (*)
s1351-tg[.]cwtapp[.]com (*)
s1355-tg[.]cwtapp[.]com (*)
s1359-tg[.]cwtapp[.]com (*)
s1360-tg[.]cwtapp[.]com (*)
s1383-tg[.]cwtapp[.]com (*)
s1386-tg[.]cwtapp[.]com (*)
s1450[.]cwtapp[.]com (*)
s1453[.]cwtapp[.]com (*)
s1470[.]cwtapp[.]com (*)
s1476[.]cwtapp[.]com (*)
s1479[.]cwtapp[.]com
s1488[.]cwtapp[.]com (*)
s1490[.]cwtapp[.]com (*)
s1504[.]cwtapp[.]com (*)
s1505[.]cwtapp[.]com (*)
s1536[.]cwtapp[.]com (*)
s1537[.]cwtapp[.]com

```
s1558[.]cwtapp[.]com (*)
s1582[.]cwtapp[.]com (*)
s1592[.]cwtapp[.]com (*)
s1606-tg[.]cwtapp[.]com
s1641[.]cwtapp[.]com (*)
s1647[.]cwtapp[.]com
s1688[.]cwtapp[.]com (*)
s1690[.]cwtapp[.]com (*)
```

Other Hosts Related to Potential Cobwebs Product Servers

List of 4 additional hosts that displayed a login page related to a Cobwebs product in the browser, as of January 30, 2026.

```
62[.]201[.]208[.]195:1210
41[.]215[.]20[.]45:3701
139[.]0[.]5[.]194:1300
4[.]233[.]111[.]135:443
```

Subdomains Related to Cobwebs' Wider Server Infrastructure

List of 69 host names that we consider to be affiliated with Cobwebs Technologies' wider server infrastructure, resolving to particular IP addresses as of January 30, 2026. Ten of them, marked with an asterisk, displayed a login page related to a Cobwebs product in the browser. We did not include them in the list of potential Cobwebs product servers because we assume that the letters "qa" in the host name refer to "quality assurance," and thus to test or staging servers.

```
tlg[.]cobwebsapp[.]com
ig[.]cobwebsapp[.]com
qa-td[.]cobwebsapp[.]com
poc[.]cobwebsapp[.]com
rest[.]cobwebsapp[.]com
cw-mgmt-hyb02-vpn[.]cobwebsapp[.]com
cw-mgmt-az-vpn[.]cobwebsapp[.]com
cobwebsapp[.]com
1300[.]cwsystem[.]com
1600[.]cwsystem[.]com
20300[.]cwsystem[.]com
2500[.]cwsystem[.]com
2700[.]cwsystem[.]com
3300[.]cwsystem[.]com
3600[.]cwsystem[.]com
3700[.]cwsystem[.]com
3800[.]cwsystem[.]com
7800[.]cwsystem[.]com
8300[.]cwsystem[.]com
```

9700[.]cwsystem[.]com
10600[.]cwsystem[.]com
12200[.]cwsystem[.]com
12300[.]cwsystem[.]com
12400[.]cwsystem[.]com
12600[.]cwsystem[.]com
13100[.]cwsystem[.]com
13200[.]cwsystem[.]com
13300[.]cwsystem[.]com
13600[.]cwsystem[.]com
14200[.]cwsystem[.]com
19600[.]cwsystem[.]com
22500[.]cwsystem[.]com
22600[.]cwsystem[.]com
32000[.]cwsystem[.]com
38000[.]cwsystem[.]com
az-man-qa01[.]cwsystem[.]com (*)
aws-auto-qa01[.]cwsystem[.]com
az-rnd-dep01[.]cwsystem[.]com
auto-qa02[.]cwsystem[.]com
az-man-qa02[.]cwsystem[.]com (*)
op-man-qa2[.]cwsystem[.]com
az-man-qa03[.]cwsystem[.]com (*)
az-rnd-dep03[.]cwsystem[.]com (*)
az-man-qa04[.]cwsystem[.]com (*)
auto-qa6[.]cwsystem[.]com
auto-qa7[.]cwsystem[.]com
op-man-qa9[.]cwsystem[.]com
az-auto-qa11[.]cwsystem[.]com
auto-qa11[.]cwsystem[.]com
auto-qa14[.]cwsystem[.]com
op-man-qa14[.]cwsystem[.]com
az-qa-mma-15-um[.]cwsystem[.]com
auto-qa21[.]cwsystem[.]com
op-man-qa31[.]cwsystem[.]com
man-qa42[.]cwsystem[.]com
man-qa100[.]cwsystem[.]com
az-man-qa130[.]cwsystem[.]com (*)
az-man-qa173[.]cwsystem[.]com
man-qa234[.]cwsystem[.]com
man-qa255[.]cwsystem[.]com
man-qa261[.]cwsystem[.]com
man-qa264[.]cwsystem[.]com
man-qa277[.]cwsystem[.]com
man-qa551[.]cwsystem[.]com
man-qa666[.]cwsystem[.]com
az-man-qa1003[.]cwsystem[.]com (*)
az-man-qa1005[.]cwsystem[.]com (*)

```
az-man-qa3000[.]cwsystem[.]com (*)
man-qa5007[.]cwsystem[.]com (*)
```

Other Hosts Related to Cobwebs' Wider Server Infrastructure

List of 10 additional hosts that we consider to be affiliated with Cobwebs Technologies' wider server infrastructure.

```
182[.]23[.]55[.]125
177[.]107[.]47[.]51
20[.]187[.]80[.]77
195[.]228[.]126[.]190
78[.]11[.]103[.]139
15[.]161[.]210[.]71
15[.]161[.]209[.]206
4[.]185[.]223[.]22
13[.]63[.]16[.]113
52[.]253[.]117[.]211
```

Trapdoor Login Page and Javascript Code

```
41[.]215[.]20[.]45:3701
41[.]215[.]20[.]45:3701/clientapp/build/main.js
```