ACLU
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION
District
of Columbia

529 14th Street NW
Ste 722
Washington, DC 20045
(202) 457-0800
www.acludc.org

Via Public FOIA Portal August 7, 2025

Joe Ruel
FOIA Officer
District of Columbia Homeland Security and Emergency Management Agency
2720 Martin Luther King Jr Ave SE, 2nd Floor
Washington, DC 20001
hsema.foia@dc.gov

Re: FOIA Request – Records regarding the District's use of Cobwebs products

Dear Officer Ruel:

This letter is a request pursuant to the D.C. Freedom of Information Act (FOIA), D.C. Code § 2-531 *et seq.*, on behalf of the American Civil Liberties Union of the District of Columbia (ACLU-DC) and its members. We request certain records regarding the District's use of software and/or products offered by Cobwebs Technologies and PenLink, Ltd. that are identified below.

I. Background

In November 2024, Washington City Paper published an article explaining that Washington D.C.'s Homeland Security and Emergency Management Agency (HSEMA) had licensed a surveillance software called "Tangles" from the intelligence firm Cobwebs Technologies ("Cobwebs") for the previous four years (2021-2024).[1] HSEMA first licensed the software months before the attack on the U.S. Capitol on January 6, 2021, and has renewed its license "for between $70,000 and $90,000 each year," resulting in a total cost to the District of $348,613.70 between 2020-2024.[2] According to an HSEMA purchase order from October 2023, HSEMA licensed Tangles "as 'a technological tool for social media threat research capabilities in support of the District of Columbia fusion center.'"[3]

Cobwebs Technologies is a cyber intelligence firm established in 2015 by former members of the Israeli Defense Forces.[4] In 2023, Cobwebs was acquired by a private equity firm and merged

[1] Mathew Schumer, *D.C. Purchased a Controversial Web-Surveillance But Won't Say How They're Using It*, Washington City Paper (Nov. 14, 2024), https://washingtoncitypaper.com/article/753352/d-c-purchased-a-controversial-web-surveillance-platform-but-wont-say-how-theyre-using-it/.

[2] *Id*.

[3] *Id*. (quoting October 2023 HSEMA purchase order).

[4] Meir Orbach, *Web intelligence startup Cobwebs acquired for $200 million by private equity firm Spire Capital*, Ctech by Calcalist (July 11, 2023), https://www.calcalistech.com/ctechnews/article/sj11008xsfh#google_vignette.

into the software company PenLink, Ltd., under which Cobwebs operates today.[5] In this FOIA Request, "Cobwebs" or "Cobwebs Technologies" refers to the company as it existed prior to the merger with PenLink, and "Cobwebs product(s)" refers to any software, technology, module, or other product that was offered by Cobwebs Technologies (including Tangles, Webloc, and Lynx), and the same or similar software, technology, module, or other product that is being or was offered by PenLink after the merger, whether under the same names or under different names.

There are three types of Cobwebs products that agencies could/can license for surveillance: Tangles, Webloc, and Lynx.[6] Tangles is a web intelligence platform that uses "real-time online content search, analysis and monitoring enhanced by alerting, case-management and reporting tools"[7] to allow "law enforcement entities to search, analyze, and monitor web-based targets using artificial intelligence."[8] Two training manuals leaked in 2024, one from 2020 and the other from 2022, supply much of what is currently known about Tangles' workflow.[9] When an "operator" (the person using Tangles) begins a search project on the Tangles interface, he or she provides the system with one type of identifying information about a person (the "target"), such as a name, phone number, email, or social media username as "[t]he investigative flow relies on information that leads to other pieces of information that leads to other pieces of information, and the connections between."[10] Once a target is identified by Tangles, operators use the system to find other accounts, posts, or groups connected to the target.[11] Tangles then visually displays potential connections to the target based on social media interactions and mutual friends.[12] Additionally, operators can set up a "monitor" (a notification) that alerts them if any number of actions occur related to the target, including if Tangles detects the target in a preselected geographic range via a social media post, a specific hashtag is used, or a number of alternative options.[13]

The second module Cobwebs offers is Webloc, a "cutting-edge location solution which automatically monitors and analyzes location-based data in any specific geographic location" to

[5] Jack Poulson, *Israeli firm taught U.S. police how to "target" BLM, Antifa, and Jan 6 protestors through social media*, All-Source Intelligence (Oct. 10, 2024), https://jackpoulson.substack.com/p/israeli-firm-taught-us-police-how.

[6] Joseph Cox, *The Company Helping the IRS Go Undercover Online*, Vice (Feb. 16, 2023), The Company Helping the IRS Go Undercover Online.

[7] *Cobwebs Technologies: Redefining the Norms of Cyber Intelligence*, Cobwebs Technologies (June 8, 2019), https://web.archive.org/web/20230207115908/https:/cobwebs.com/press-releases/cobwebs-technologies-redefining-the-norms-of-cyber-intelligence/.

[8] Schumer, *supra* n. 1.

[9] Poulson, *supra* n. 5, *see* documents linked on webpage "*Tangles: QuickStart Guide*, Cobwebs Technologies (2020)" and "*Tangles: Work Flow and Methodology*, Cobwebs Technologies (2022)."

[10] *Id.*, *see* document linked on webpage "*Tangles: Work Flow and Methodology*, Cobwebs Technologies (2022)," at 3.

[11] *Id.* at 5-6.

[12] *Id.* at 8-11.

[13] *Id.* at 22-25.

retrieve geolocation extractions.[14] Geolocation extraction refers to the process of "identifying the physical locations of devices and individuals based on information such as geographic coordinates and Internet Protocol (IP) addresses."[15] Webloc "uses commercial data purchased from [data] brokers to identify unique mobile advertising IDs assigned to smartphones and mobile devices" that "can be used to track a person's movements."[16] These data brokers are companies that take advantage of the "explosion of data caused by smartphones and high-speed internet service" to "assemble[], analyze[], and sell[] data from mobile apps, cookies, and other sources to create detailed dossiers of millions of Americans" used to identify advertising IDs.[17] An advertising ID is a unique combination of numbers and letters that "acts as a unique identifier for mobile devices in the advertising marketing ecosystem."[18] Data companies sell information "that helps to link mobile device identifiers"—unique identifying codes that all smartphones have—"to email addresses, phone numbers, names and postal addresses" that Webloc then draws on to provide the exact locations of smartphones and the information associated with their owners, including age, gender, and interests.[19] This information is displayed "on a simple and map-centric interface that allows operators to conduct a map-based and visual investigation."[20]

The third module Cobwebs offers is Lynx, a program that provides a global network of proxies that allows analysts to "join darknet forums, hacker communities, and other platforms without their cover being blown" and is offered only to government customers.[21] The "darknet" refers to any intentionally hidden network that requires a special configuration or specific credentials to access.[22] These hidden sites frequently host discussion boards where illicit activity

[14] Sam Biddle & Ryan Devereaux, *Texas State Police Purchased Israeli Phone-Tracking Software For "Border Emergency,"* The Intercept (July 26, 2023), https://theintercept.com/2023/07/26/texas-phone-tracking-border-surveillance/.

[15] Cameron Hashemi-Pour, *What is geolocation? Explaining how geolocation data works*, TechTarget (Aug. 15, 2024), https://www.techtarget.com/searchmobilecomputing/definition/What-is-geolocation.

[16] Robert Skvarla*, Cobwebs Spy Software Locks Onto Protestors: Israeli Social Media Mining Contract with Homeland Security Revealed Israeli Firm "Cobwebs" Linked to 2020 Protests, Provides Monitoring Services to Homeland Security for Tracking Dissenters*, Unicorn Riot (June 14, 2024), https://unicornriot.ninja/2024/cobwebs-spy-software-locks-onto-protesters-israeli-social-media-mining-contract-with-homeland-security-revealed/.

[17] Elizabeth Goitein & Emile Ayoub, *Data Brokers Are Running Wild, and Only Congress Can Rein Them In*, Brennan Center for Justice (Feb. 13, 2024), https://www.brennancenter.org/our-work/analysis-opinion/data-brokers-are-running-wild-and-only-congress-can-rein-them.

[18] Francesca D'Annunzio, *Everything Is Bigger In Texas – Including State Police Contracts For Surveillance Tech*, ReformAustin (Dec. 26, 2024), https://www.reformaustin.org/trib/everything-is-bigger-in-texas-including-state-police-contracts-for-surveillance-tech/.

[19] Biddle & Devereaux, *supra* n. 14.

[20] Roscoe, *The LAPD Is Using Controversial Mass Surveillance Tracking Software, Vice (Nov. 29, 2023), https://www.vice.com/en/article/the-lapd-is-using-controversial-mass-surveillance-tracking-software/*.

[21] Cox, *supra* n. 6.

[22] Alex Vakulov, *Dark Web Secrets: What Is It And Why Should You Care*, Forbes (Feb 04, 2025), https://www.forbes.com/sites/alexvakulov/2025/02/04/dark-web-secrets-what-it-is-and-why-you-should-care/.

is discussed and marketed.[23] Operators can then feed information gathered from these sites into Tangles and Webloc to facilitate the collection and analysis of the darknet information.[24]

Since 2020, various U.S. state and federal agencies have entered into agreements with Cobwebs to purchase one or more of these three modules, including but not limited to a 2020 purchase of Tangles, Webloc, and Lynx for $181,000 by the Internal Revenue Service (IRS),[25] a 2021 purchase of Tangles for $198,000 by the Texas Department of Public Safety,[26] a 2022 purchase of Tangles for $226,060 by Immigration and Customs Enforcement,[27] a 2022 purchase of Tangles and Webloc for nearly $200,000 by the Los Angeles Police Department,[28] and the aforementioned purchase of Tangles by the District’s HSEMA from at least 2020-2024.[29]

Other than to “monitor social media threats,” little is known about how Tangles and potentially other technologies offered by Cobwebs were and/or are being used in D.C.[30] The 2020 Tangles training manual shows a page of results that included the then Twitter username of black-led activist group Freedom Fighters DC (@FFDC2020), the Twitter username of an anonymous independent journalist who was shot in the leg by DC police on August 29, 2020 (@rawsmedia), and the hashtag #DefundDCPolice as examples of types of targets that can be monitored.[31] The 2022 Tangles training manual continued the pattern of featuring individuals connected with D.C. by focusing on “Dallas-based real-estate agent and January 6th protester Brian Miller.”[32] The 2022 manual also made clear that “[t]he profiles used were examples to showcase how the Tangles platform can be utilized in an investigation using the advanced capabilities of search, analysis, and monitoring of open-source data,” noting as a disclaimer that “[t]he profiles mentioned in this report were found from an Open Source Intelligence (OSINT) perspective” and “[n]o conclusive evidence relating to criminal activity has been found and they should all be presumed innocent.”[33]

[23] *Id.*
[24] *See* Cox, *supra* n. 6.
[25] *Id.*
[26] Biddle & Devereaux, *supra* n. 14.
[27] Cox, *supra* n. 6.
[28] Roscoe, *supra* n. 20.
[29] Schumer, *supra* n. 1.
[30] *Id.*
[31] *See* Poulson, *supra* n. 5, *see also* document linked on webpage “*Tangles: QuickStart Guide*, Cobwebs Technologies (2020)” at 12; *see also* Jess Arnold, *‘The work is just starting’ ' | Here’s Freedom Fighters DC’s plan for action beyond the protests*, WUSA9 (June 9, 2020), https://www.wusa9.com/article/news/local/protests/freedom-fighters-dc-plans-for-action-beyond-protests/65-e7da47eb-bcd1-4253-b9c1-abce7e468475.
[32] Poulson, *supra* n. 5.
[33] Poulson, *supra* n. 5, *see* document linked on webpage “*Tangles: Work Flow and Methodology*, Cobwebs Technologies (2022),” at 27.

In 2021, Meta released a report revealing that it had removed about 200 accounts that allegedly were operated by Cobwebs and its customers.[34] According to Meta, these accounts were "engaged in social engineering to join closed communities and forums and trick people into revealing personal information."[35] Not only did these accounts target individuals as part of law enforcement activities, but Meta also "observed frequent targeting of activists, opposition politicians and government officials in Hong Kong and Mexico" by these Cobwebs-operated accounts.[36]

II. Records Requested

The ACLU-DC requests any and all documents containing policies, procedures, guidelines, manuals, agreements, memoranda, or orders that pertain to the operation and function of any "Cobwebs product" (as defined above on pg. 2), including but not limited to:

1. Any and all documents regarding the purchase, leasing, or licensing of a Cobwebs product, including but not limited to any communications, contracts, invoices, statements of work, purchase orders, and correspondence between HSEMA and Cobwebs or PenLink for Tangles or any other Cobwebs product.

2. Any and all documents reflecting policies, procedures, or instructions for District employees using any Cobwebs product. This includes but is not limited to any user guides, reference sheets, manuals, email instructions or online walkthroughs/trainings discussing how to operate Tangles, Webloc, Lynx, or any other Cobwebs product as well as any document governing how these policies, procedures, or instructions are enforced.

3. Any and all documents discussing the 2020 and 2022 leaked Tangles manuals and training of District employees regarding the use of Tangles.

4. Any and all documents regarding the training provided to staff with access to any Cobwebs product, including but not limited to any documents relating to training on the legal and ethical requirements of using a Cobwebs product and any technical training that pertains to operating those modules. This includes any and all documents regarding the process/procedure, legal standard, and/or supervisory approval for government personnel to access or analyze outputs from any Cobwebs product.

[34] Mike Dvilyanski, David Agranovich, & Nathaniel Gleicher, *Threat Report on the Surveillance-for-Hire Industry*, Meta, 6-8 (Dec. 16, 2021), https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

[35] *Id*. at 7-8.

[36] *Id*. at 8.

5. Any and all documents regarding the past, current, or future capabilities of artificial intelligence, facial recognition, or analytic technology or software as part of, or in connection with, any Cobwebs product, including but not limited to any policies, procedures, or trainings related to the use of such technologies and capabilities as part of using or being able to access a Cobwebs product.

6. Any and all documents regarding the District's past, current, or future use of purchased commercial data, mobile advertising IDs, or other sources of information in connection with any Cobwebs product, including but not limited to any documents regarding how purchased commercial data, mobile advertising IDs, or other sources of information are used to track an individual or an entity's geolocation.

7. Any and all documents discussing, describing, or showing knowledge of Cobwebs' or PenLink's relationship with Meta, including but not limited to any documents containing an acknowledgment of or pertaining to Meta's decision to remove accounts operated by Cobwebs and/or its report of Cobwebs' use to target activists, opposition politicians, and governmental officials.

8. Any and all documents discussing, describing, or setting out any District policy or practice regarding retaining or storing data gathered by any Cobwebs product. This includes but is not limited to documents regarding how long targets are monitored, what is done with the information after an investigation, and who is responsible for ensuring compliance with any such policies or practices.

9. Any other documents that can be located in HSEMA machine-searchable records by searching for the terms "Cobwebs," "PenLink," "Tangles," "Webloc," and "Lynx."

We believe the requested documents are public records and not exempt from disclosure under the D.C. FOIA. Please note that we do *not* seek any confidential information regarding employees, and any such information may be redacted from any responsive document.

If you determine that some or all of the records are exempt, you must provide a written explanation including a reference to the specific statutory exemption on which you rely. D.C. Code § 2-533(a). If a segregable portion of any record is not exempt, you must provide those portions along with your explanation of the exemption. D.C. Code § 2-534(b). We reserve the right to appeal any such decision.

III. Fee Waiver Requested

We request a fee waiver pursuant to D.C. Code § 2-532(b), which authorizes you to waive or reduce any fee for searching and reproducing records if "furnishing the information can be considered as primarily benefiting the general public." ACLU-DC is a nonprofit public interest organization with limited resources, dedicated to the protection of civil rights and civil liberties. The public is the primary beneficiary of the ACLU-DC's work to protect fundamental rights, whether by litigation, legislative advocacy, or publication. It is on this ground that federal, state, and local agencies, as well as courts, generally grant waivers of fees for ACLU-DC FOIA requests. The present request satisfies the statutory criteria for a fee waiver because the ACLU-DC intends to understand and analyze how the District is using any Cobwebs product to determine its impact on the privacy interests and civil and constitutional rights of D.C. residents.

If you determine no waiver is appropriate, and if the proposed fee is greater than $25.00, we ask that you notify us prior to fulfilling the above requests.

Please furnish all applicable records to Aditi Shah by emailing them to ashah@acludc.org. If you have questions, please contact me at ashah@acludc.org.

We look forward to your reply to this records request within 15 business days, as required by D.C. Code § 2-532(c). Thank you for your prompt attention to this matter.

Sincerely,

/s/ *Aditi Shah*
Aditi Shah
Staff Attorney
American Civil Liberties Union Foundation
of the District of Columbia
529 14th Street NW, Suite 722
Washington, D.C. 20045