



Written by [Veronika Kyrylenko](#) on September 4, 2025

ICE Reactivates Contract With Israeli-linked Spyware Firm Paragon

U.S. Immigration and Customs Enforcement (ICE) has reactivated a \$2 million spyware contract with Paragon Solutions, an Israeli-founded firm now owned by a U.S. private equity group. The move lifts a Biden-era freeze and signals a deeper embrace of invasive surveillance tools in domestic immigration enforcement.

It is also only the latest sign of how far the federal government's surveillance apparatus has grown under the banner of "immigration enforcement." ICE has become one of its most powerful nodes — a conduit through which cutting-edge spyware, data analytics, and AI-driven tools are deployed inside U.S. borders.



Paragon/LinkedIn

Contract Reborn

On September 1, journalist Jack Poulson, citing the official procurement note, [reported](#) that ICE quietly lifted a stop-work order on the Paragon contract. The order had been in place since October 2024, after the Biden administration paused the deal under [Executive Order 14093](#). That order barred agencies from buying foreign spyware tied to human rights abuses.

Paragon

Paragon is an Israeli spyware company founded in 2019 by veterans of Israel's cyberwarfare Unit 8200, the equivalent of the U.S. National Security Agency (NSA). Among the early backers is Prime Minister Ehud Barak, a longtime political heavyweight and known associate of Jeffrey Epstein. From the start, it marketed itself as the "ethical" alternative to [Pegasus](#), another notorious Israeli spyware.

[Citizen Lab](#) reports that by 2021 Paragon had launched a U.S. subsidiary and staffed it with former CIA, Air Force, and defense contractor officials. That gave it a foothold in Washington. Within two years, ICE had signed a \$2 million contract for its spyware; U.S. Special Operations Command disclosed more than \$11 million in related purchases.

In late 2024, ownership shifted. All shares in Paragon Israel were transferred to Paragon Parent Inc., a new Delaware corporation. The deal, [reportedly](#) led by Florida-based private equity firm AE Industrial Partners, was valued at \$500 million up front, with another \$400 million tied to performance goals. Soon after, Paragon was folded into [REDLattice](#), a Virginia contractor already known for offensive cyber tools. U.S. Securities and Exchange Commission (SEC) filings show REDLattice's parent company then added ex-CIA and U.S. Army chiefs to its board.

Once Paragon became "American-owned," ICE lifted the freeze on its spyware contract. In effect, the



Written by [Veronika Kyrylenko](#) on September 4, 2025

U.S. government blocked the deal when the company was Israeli but allowed it once Americans — many with intelligence and military ties — took control. The spyware itself did not change, only the ownership structure, and it is far from clear how much influence Israeli intelligence veterans still wield inside the company.

Graphite

Graphite is Paragon’s flagship spyware. Unlike Pegasus, which can take full control of a phone, Graphite focuses on breaking in to encrypted messaging apps. It can pull data from WhatsApp, Signal, and iMessage without seizing the entire device.

Investigators have shown that Graphite often relies on “zero-click” exploits. These attacks require no action from the target. Once inside, the spyware extracts texts, call logs, photos, videos, and even microphone input. All of it is sent to remote servers controlled by the operator. Citizen Lab’s [forensic report](#) from this June confirmed the tool had been deployed against journalists in Europe. Their devices were fully updated yet still compromised until Apple patched the flaw in iOS 18.3.1.

This technical profile explains why Graphite is so attractive to governments. It is stealthy, precise, and hard to detect. But its use has raised alarms well beyond Israel and the United States.

Italian Affair

Paragon’s branding as an “ethical” alternative came under direct challenge in Italy. In early 2025, Italian journalists revealed that their phones had been hacked with Graphite. *The Guardian* [reported](#) in January:

Nearly 100 journalists and other members of civil society using WhatsApp, the popular messaging app owned by Meta, were targeted by spyware owned by Paragon Solutions, an Israeli maker of hacking software.

Among them were Italian reporter *Ciro Pellegrino* of *Fanpage.it*, and Libyan activist *Husam El Gomati*, who was based in Sweden.

Italy’s parliamentary intelligence oversight body, COPASIR, [later confirmed](#) that both domestic and foreign intelligence agencies had activated contracts with Paragon in 2023 and 2024. The report said that the government used Graphite in a small number of carefully targeted cases. It claimed legal authorization, and said it used the spyware for national security and anti-immigration operations.

Paragon said it ended its Italian contracts after Rome refused its offer to investigate possible misuse. Italian officials rejected that version, and said they had already suspended the deals on national security grounds.

Human rights groups, including Amnesty International, warned that such invasive tools, deployed covertly against the media and aid workers, “confirmed widespread use of unlawful surveillance” and thus posed a grave threat to democratic norms.

The Expanding Net

ICE’s spyware deal with Paragon is just one thread in a sprawling surveillance web. A 2022 [report](#) from Georgetown Law’s Center on Privacy and Technology details how ICE pulls in everything from DMV photos to utility data — often without warrants or oversight — compiling dossiers on millions:



Written by [Veronika Kyrylenko](#) on September 4, 2025

By reaching into the digital records of state and local governments and buying databases with billions of data points from private companies, ICE has created a surveillance infrastructure that enables it to pull detailed dossiers on nearly anyone, seemingly at any time.

Now ICE's reach is getting a high-tech jolt — and a massive budget surge. Trump's "[One Big Beautiful Bill](#)," signed in July, funneled over \$100 billion into ICE through 2029, dwarfing its former \$8 billion annual budget. The measure pours [billions](#) into modern surveillance technologies. Those include biometric systems and AI-driven monitoring tools — the digital muscle behind a rapidly expanding enforcement state. Amid that spending surge, ICE handed Palantir a \$30 million contract to build [ImmigrationOS](#). The system performs real-time surveillance, deportation tracking, and database fusion at scale. For many, Palantir, seeded by the CIA and co-founded by Peter Thiel — Trump's longtime ally and megadonor — embodies the concept of the Deep State in silicon form.

We would be naive — dangerously so — to assume that these tools will target only immigrants. As Congress keeps inflating surveillance budgets and reauthorizing the Foreign Intelligence Surveillance Act (FISA), systems like ImmigrationOS and Graphite can and will spill into domestic policing.

Related:

[Palantir to Build Centralized Database on Americans](#)



Subscribe to the New American

Get exclusive digital access to the most informative,
non-partisan truthful news source for patriotic Americans!

Discover a refreshing blend of time-honored values, principles and insightful perspectives within the pages of "The New American" magazine. Delve into a world where tradition is the foundation, and exploration knows no bounds.

From politics and finance to foreign affairs, environment, culture, and technology, we bring you an unparalleled array of topics that matter most.



Subscribe

What's Included?

- 24 Issues Per Year
- Optional Print Edition
- Digital Edition Access
- Exclusive Subscriber Content
- Audio provided for all articles
- Unlimited access to past issues
- Coming Soon! Ad FREE
- 60-Day money back guarantee!
- Cancel anytime.