

On September 1, 2025, media reported that U.S. Immigrations and Customs Enforcement (ICE) was lifting a stop work order that had paused a two million USD contract with spyware vendor Paragon Solutions. The government issued the stop work order in October 2024 — one week after the news broke about the contract — to ensure it complied with Executive Order 14093 (EO). This EO prohibits U.S. federal agencies from using commercial spyware tools that “pose significant counterintelligence or security risks [or] significant risks of improper use by a foreign government or foreign person, including to target Americans or enable human rights abuses.”

Reactivation of the contract does not necessarily indicate a review was completed, and activists are still trying to verify what happened. It’s not clear from publicly available information which technologies or services are involved. What we do know is that there is evidence that Paragon’s flagship spyware, Graphite, has been misused to violate human rights around the world. The technology can reportedly covertly access encrypted apps on a device even when you don’t click on anything. ICE already owns and has access to a wide range of surveillance and monitoring technology. Now that the stop work order has been lifted, we fear ICE agents may use Graphite as they patrol U.S. communities.

Why ICE + Paragon = a problem

Paragon’s global record should have triggered multiple red flags under EO 14093. Investigations by WhatsApp and Citizen Lab revealed that Italian authorities used Graphite to target at least three journalists and two individuals working in organizations involved in rescuing refugees at sea in Europe. A campaigner for migrants in Libya is also suspected of being a Graphite target. In the U.S., individuals doing similar work, including migrants, organizers, lawyers, and journalists documenting state abuse of power, already face intensive surveillance.

Members of the U.S. Congress have formally asked the Department of Homeland Security how the Paragon contract satisfies the safeguards the EO sets forth. Last week, in a letter to the Department of Homeland Security (DHS), representatives warned that deploying Paragon’s spyware could violate the First Amendment’s guarantees of free speech and assembly and the Fourth Amendment’s protections against warrantless searches. Under U.S. law, the Fourth Amendment, Electronic Communications Privacy Act (ECPA), and Foreign Intelligence Surveillance Act (FISA) set strict limits on government surveillance and require judicial authorization for searches, with some exceptions.

Any use of surveillance technology by the U.S. government also raises serious concerns about how the government handles the data it obtains — where it is stored, who can access it, and how long it is retained (the Privacy Act and the E-Government Act generally apply to the collection, storage, and use of personal information by U.S. agencies). ICE and its sister agency, Customs and Border Protection (CBP), have faced criticism for using digital-extraction tools like Cellebrite to extract information from travelers’ devices under the border search exception. The practice has allowed people’s sensitive personal information — including potentially attorney-client privileged communications and materials protected by the First Amendment — to be extracted and stored for years and shared across agencies. This has created a vast pool of information vulnerable to misuse or unauthorized access.

With the use of commercial spyware, there is an added cybersecurity threat: by purchasing and deploying these tools, the U.S. risks feeding the global exploits market that sustains the spyware industry. The same vulnerabilities that Graphite exploits can be used by other threat actors and governments, leading to further proliferation of invasive tools that

circulate with little control, ultimately undermining digital security and exposing critical systems and individuals alike to attack.

The Graphite case fits an alarming pattern: ICE has steadily expanded its digital surveillance arsenal in recent years, adding tools to spy, extract, store, and analyze vast amounts of personal data — including from surveillance data contractors such as Palantir, whose platforms underpin mass data collection for immigration enforcement. The procurement of spyware with such intrusive capacities could supercharge the agency's ability to engage in targeted surveillance, raising fresh human rights and national security concerns. How will it be deployed? What guidelines will govern its use? How will ICE ensure accountability for abuse?

Access Now and partners already raised these questions in an open letter we sent to AE Industrial Partners and Paragon on June 19, 2025. At the time of publishing, we have not received an official response.

What needs to happen now

We need urgent action to ensure that federal agencies do not use spyware in violation of U.S. laws and fundamental human rights. Access Now has successfully engaged Congress for years to urge action against foreign commercial spyware's threat to human rights defenders around the world and to U.S. national security. To its credit, Congress has passed into law several pieces of legislation that mandate transparency on spyware attacks and created policy levers to punish spyware violators. Now, Congress must act again, exercising its oversight authority to scrutinize ICE's contract with Paragon, and all similar contracts, to prevent spyware abuse.

In addition, those impacted should take action to hold perpetrators of abuse accountable, including tech companies whose platforms are exploited to deliver spyware.

Here's what we recommend:

- ? Immediate suspension of contracts: DHS should halt all spyware contracts until the DHS Office of Inspector General (OIG) independent verification confirms compliance with EO 14093 and includes a comprehensive human rights impact assessment.**
- ? Transparency first: DHS and ICE must disclose all risk assessments, vendor communications, and oversight findings linked to Paragon and Graphite.**
- ? Congressional oversight: Congress should exercise its oversight authority and scrutinize ICE's contract, require public reporting on any use or testing of Graphite, and hold hearings on spyware procurement across federal agencies.**
- ? Legislative reform: Congress should codify EO 14093 to explicitly prohibit domestic use of spyware sold by vendors tied to previous human-rights abuses and national security threats.**
- ? Ramp up the heat: Individuals and businesses, such as people who have been hacked and tech companies whose infrastructure and services have been targeted for attack, should challenge the unlawful use of spyware technologies, including through lawsuits.**