

They Exposed an Israeli Spyware Firm. Now the Company Is Badgering Them in Court.

Shawn Musgrave : 5-6 minutes : 5/6/2024

For years, cybersecurity researchers at Citizen Lab have monitored Israeli spyware firm NSO Group and its banner product, Pegasus. In 2019, Citizen Lab [reported](#) finding dozens of cases in which Pegasus was used to target the phones of journalists and human rights defenders via a WhatsApp security vulnerability.

Now NSO, which is [blacklisted](#) by the U.S. government for selling spyware to repressive regimes, is trying to use a lawsuit over the WhatsApp exploit to learn “how Citizen Lab conducted its analysis.”

The lawsuit, filed in U.S. federal court in 2019 by WhatsApp and Meta (then Facebook), [alleges](#) that NSO sent Pegasus and other malware to approximately 1,400 devices across the globe. For more than four years, NSO has failed repeatedly to get the case thrown out.

With the lawsuit now moving forward, NSO is trying a different tactic: demanding repeatedly that Citizen Lab, which is based in Canada, hand over every single document about its Pegasus investigation. A judge denied NSO’s latest attempt to get access to Citizen Lab’s materials last week.

Providing its raw work to NSO, Citizen Lab’s lawyers [argued](#), would “expose individuals already victimized by NSO’s activities to the risk of further harassment, including from their own governments” and chill their future work. (NSO declined to comment about the lawsuit.)

NSO has mounted an [aggressive campaign](#) to rehabilitate its image in recent years, particularly since being blacklisted in 2021. Last November, following the October 7 Hamas attacks, the firm [requested a meeting](#) with the State Department to discuss Pegasus as a “critical tool that is used to aid the ongoing fight against terrorists.”

The company has faced other lawsuits in U.S. courts over Pegasus, including ongoing suits brought by [Salvadoran journalists](#), [Apple](#), and [Hanan Elatr Khashoggi](#), the widow of murdered journalist Jamal Khashoggi. These lawsuits also rely on Citizen Lab’s research, to varying degrees.

So far, the WhatsApp lawsuit — which NSO recently called “a one-sided ‘show’ trial” in the making — has not gone particularly well for the spyware firm. At first, NSO argued it was entirely immune from being sued in American courts, which a federal appeals court [roundly rejected](#) in 2021 and the U.S. Supreme Court [declined](#) to consider in early 2023.

Next, NSO argued the lawsuit should have been filed in Israel instead of the U.S. District Court for the Northern District of California, where both WhatsApp and Meta (which also owns WhatsApp) have their headquarters. Judge Phyllis Hamilton [rejected](#) that argument too.

In perhaps the biggest blow to NSO, earlier this year Hamilton [ordered](#) the company to disclose its software code, not just for Pegasus but also for “any NSO spyware targeting or directed at WhatsApp servers, or using WhatsApp in any way to access target devices.”

During discovery, NSO has already obtained thousands of documents from Meta and WhatsApp regarding Citizen Lab’s investigation into Pegasus. Regardless, NSO has tried and failed twice to use the lawsuit to get more information directly from Citizen Lab, which is based at the University of Toronto. In March, Hamilton [denied](#) NSO’s first request to send a cross-border demand — a “letter rogatory” — to her counterparts at the Ontario Superior Court of Justice.

NSO tried again last month. “The evidence Plaintiffs themselves have produced about Citizen Lab’s investigation is incomplete and inadequate,” its lawyers [argued](#), because it did not show “how Citizen Lab conducted its analysis or came to its conclusions” that Pegasus was used to target individuals in civil society, as opposed to criminals or terrorists.

“We are pleased the court has recognized that NSO Group’s request for information was overbroad and not necessary.”

Citizen Lab opposed NSO’s demands on numerous grounds, particularly given “NSO’s animosity” toward its research.

In the latest order, Hamilton concluded that NSO’s demand was “plainly overbroad.” She left open the possibility for NSO to try again, but only if it can point to evidence that specific individuals that Citizen Lab categorized as “civil society” targets were actually involved in “criminal/terrorist activity.”

“We are pleased the court has recognized that NSO Group’s request for information was overbroad and not necessary at this time to resolve the disputed issues,” Citizen Lab’s director, Ronald Deibert, told The Intercept.