Judge rules NSO Group is liable for spyware hacks targeting 1,400 WhatsApp user devices

By Suzanne Smalley

Published: 2024-12-21 · Archived: 2026-04-05 16:20:02 UTC

The developer of the powerful Pegasus spyware was found liable on Friday for its role in the infection of devices belonging to 1,400 WhatsApp users.

The precedent-setting ruling from a Northern California federal judge could lead to massive damages against NSO Group, whose notorious spyware has been reportedly used, and often abused, by a roster of anonymous government clients worldwide.

No court has ever before held the company liable for abuses despite its spyware being found on hundreds of phones belonging to activists, journalists and other members of civil society. The company has long stated that its tools can only be used by national security officials and law enforcement officers investigating intelligence matters and crimes.

Meta-owned WhatsApp sued in 2019, alleging NSO Group had found a bug in its systems and used it to install spyware on some users' devices. Journalists, human rights activists, political dissidents, diplomats and senior foreign government officials, frequent targets of Pegasus, were among the WhatsApp victims.

The Israeli spyware maker repeatedly tweaked the exploit to penetrate defenses WhatsApp put in place over the course of two years, the WhatsApp lawsuit says.

Northern California federal judge Phyllis Hamilton determined that the NSO Group violated the federal Computer Fraud and Abuse Act (CFAA) and California's Comprehensive Computer Data Access and Fraud Act (CDAFA) for enabling the hacks. The judge also found NSO Group liable for breach of contract for violating WhatsApps' terms of service.

"After five years of litigation, we're grateful for today's decision," WhatsApp said in a statement. "NSO can no longer avoid accountability for their unlawful attacks on WhatsApp, journalists, human rights activists and civil society."

"With this ruling, spyware companies should be on notice that their illegal actions will not be tolerated."

A spokesperson for the NSO Group did not immediately respond to a request for comment.

Advocates for spyware victims applauded the decision.

"This is the first successful case against NSO Group where NSO was found liable for compromising the digital security infrastructure that millions of people rely on with Pegasus spyware," said Natalia Krapiva, senior tech legal counsel at Access Now.

“While the court still has to determine the damages that the NSO should pay, the partial summary judgment is a major win not just for WhatsApp, whose servers were targeted by NSO, but for hundreds of victims around the world whose lives have been destroyed by Pegasus and other spyware.”

Krapiva added that spyware companies around the world should take notice that “the time of impunity is over and they will be brought to justice for undermining the security of our devices and platforms, as well as our human rights.”

In her ruling, the judge lambasted NSO Group for repeatedly failing to produce complete Pegasus source code despite a court order requiring that it be turned over.

NSO submitted source code that could only be viewed by Israeli citizens present in Israel, the judge said in her order, citing NSO’s failure to produce its full source code in an accessible manner as a major reason she decided to grant WhatsApps’ request for sanctions.

The judge said that NSO Group used a “Whatsapp Installation Server,” or WIS, which allowed their clients to send “cipher” files with “installation vectors” allowing surveillance of targets.

NSO Group appears to “fully acknowledge that the WIS sent messages through Whatsapp servers that caused Pegasus to be installed on target users’ devices, and that the WIS was then able to obtain protected information by having it sent from the target users, through the Whatsapp servers, and back to the WIS,” the judge said.

Senior NSO executives deposed in the case admitted in sworn testimony to developing the exploits used in the WhatsApp hacks. Recently unsealed court filings also show that WhatsApp’s security team repeatedly blocked Pegasus intrusions only to see NSO develop new malware to overcome their efforts.

The high-profile lawsuit offered a rare glimpse into the inner workings of a shadowy spyware manufacturer whose executives admitted in depositions that, contrary to past assertions, NSO Group does in fact control data extraction from the targets’ devices and the process for embedding the spyware on them.

“NSO’s customers’ role is minimal,” one WhatsApp filing says, citing a senior executive’s deposition. “NSO controls every aspect of the data retrieval and delivery process through its design of Pegasus.”

The spyware manufacturer had fought to keep the depositions from being publicly released, but the judge overruled the company, ordering the filings to be unsealed last month.

Evidence from the case also shows that NSO Group continued to develop new malware that infected victims via their WhatsApp accounts even after the messaging platform sued the spyware company for allegedly violating federal anti-hacking laws.

Arguments to determine damages will begin in March, according to the court docket.

Suzanne Smalley

is a reporter covering digital privacy, surveillance technologies and cybersecurity policy for The Record. She was previously a cybersecurity reporter at CyberScoop. Earlier in her career Suzanne covered the Boston Police Department for the Boston Globe and two presidential campaign cycles for Newsweek. She lives in Washington with her husband and three children.
