F.B.I. Told Israel It Wanted Pegasus Hacking Tool for Investigations

A 2018 letter from the bureau to the Israeli government is the clearest documentary evidence to date that the agency weighed using the spyware for law enforcement operations.


By Mark Mazzetti and Ronen Bergman
May 12, 2022

WASHINGTON — The F.B.I. informed the Israeli government in a 2018 letter that it had purchased Pegasus, the notorious hacking tool, to collect data from mobile phones to aid ongoing investigations, the clearest documentary evidence to date that the bureau weighed using the spyware as a tool of law enforcement.

The F.B.I.'s description of its intended use of Pegasus came in a letter from a top F.B.I. official to Israel's Ministry of Defense that was reviewed by The New York Times. Pegasus is produced by an Israeli firm, NSO Group, which needs to gain approval from the Israeli government before it can sell the hacking tool to a foreign government.

The 2018 letter, written by an official in the F.B.I.'s operational technology division, stated that the bureau intended to use Pegasus "for the collection of data from mobile devices for the prevention and investigation of crimes and terrorism, in compliance with privacy and national security laws."

The Times revealed in January that the F.B.I. had purchased Pegasus in 2018 and, over the next two years, tested the spyware at a secret facility in New Jersey.

Since the article's publication, F.B.I. officials have acknowledged that they considered deploying Pegasus but have emphasized that the bureau bought the spying tool mainly to test and evaluate it — partly to assess how adversaries might use it. They said the bureau never used the spyware in any operation.

During a congressional hearing in March, the F.B.I. director, Christopher A. Wray, said the bureau had bought a "limited license" for testing and evaluation "as part of our routine responsibilities to evaluate technologies that are out there, not just from a perspective of could they be used someday legally, but also, more important, what are the security concerns raised by those products."

"So, very different from using it to investigate anyone," he said.

The Times revealed that the F.B.I. had also received a demonstration by NSO of a different hacking tool, Phantom, that can do what Pegasus cannot — target and infiltrate U.S. cellphone numbers. After the demonstration, government lawyers spent years debating whether to purchase and deploy Phantom. It was not until last summer that the F.B.I. and the Justice Department decided not to deploy NSO hacking tools in operations.

The F.B.I. has paid approximately $5 million to NSO since the bureau first purchased Pegasus.

The Times has sued the F.B.I. under the Freedom of Information Act for bureau documents related to the purchase, testing and possible deployment of NSO spyware tools. During a court hearing last month, a federal judge set a deadline of Aug. 31 for the F.B.I. to produce all relevant documents or be held in contempt. Government lawyers said the bureau thus far had identified more than 400 pages of documents that were responsive to the request.

The F.B.I. letter to NSO, dated Dec. 4, 2018, stated that "the United States government will not sell, deliver or otherwise transfer to any other party under any condition without prior approval of the government of Israel."

Cathy L. Milhoan, an F.B.I. spokeswoman, said the bureau "works diligently to stay abreast of emerging technologies and tradecraft."

"The F.B.I. purchased a license to explore potential future legal use of the NSO product and potential security concerns the product poses," she continued. "As part of this process, the F.B.I. met requirements of the Israeli Export Control Agency. After testing and evaluation, the F.B.I. chose not to use the product operationally in any investigation."

The Times article in January revealed that the C.I.A. in 2018 arranged and paid for the government of Djibouti to acquire Pegasus to assist its government in counterterrorism operations, despite longstanding concerns about human rights abuses there.

Pegasus is a so-called zero-click hacking tool — it can remotely extract everything from a target's mobile phone, including photos, contacts, messages and video recordings, without the user having to click on a phishing link to give Pegasus remote access. It can also turn phones into tracking and secret recording devices, allowing the phone to spy on its owner.

NSO has sold Pegasus to dozens of countries, which have used the spyware as part of investigations into terrorist networks, pedophile rings and drug kingpins. But it has also been abused by authoritarian and democratic governments alike to spy on journalists, human rights activists and political dissidents.

On Tuesday, the chief of Spain's intelligence agency was ousted after recent revelations that Spanish officials both deployed and were victims of Pegasus spyware.

The firing of the official, Paz Esteban, came days after the Spanish government said that the cellphones of senior Spanish officials, including Prime Minister Pedro Sánchez and Defense Minister Margarita Robles, had been penetrated last year by Pegasus. It was also revealed recently that the Spanish government had used Pegasus to penetrate the cellphones of Catalan separatist politicians.

Israel has used the tool as a bargaining chip in diplomatic negotiations, most notably in the secret talks that led to the so-called Abraham Accords that normalized relations between Israel and several of its historic Arab adversaries.

In November, the Biden administration put NSO and another Israeli firm on a "blacklist" of firms that are prohibited from doing business with American companies. The Commerce Department said the companies' spyware tools had "enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to

silence dissent."

Mark Mazzetti reported from Washington, and Ronen Bergman from Tel Aviv.

Mark Mazzetti is a Washington investigative correspondent, and a two-time Pulitzer Prize winner. He is the author of "The Way of the Knife: the C.I.A, a Secret Army, and a War at the Ends of the Earth." @MarkMazzettiNYT

Ronen Bergman is a staff writer for The New York Times Magazine, based in Tel Aviv. His latest book is "Rise and Kill First: The Secret History of Israel's Targeted Assassinations," published by Random House.

A version of this article appears in print on , Section A, Page 7 of the New York edition with the headline: Letter Shows F.B.I. Weighed Using Spyware