



# Pegasus

& the Phantom Menace It Left Behind

Southwest Cyber Security  
Forum

# What is Pegasus?

**Pegasus is Israeli surveillance software developed by the NSO Group used by governments worldwide for both good and evil. It started as a chicken co-op.**

- **Has been sold to global law enforcement & intelligence agencies since 2011**
- **Takes ALL the data from an iPhone, Android, Blackberry or Symbian phone – the phone’s location, every message (email and text), contacts, photographs, document, and download, including encrypted communication**
- **Real time monitoring of all your activities**
- **Can seize control of a smartphone’s camera and microphone – “room tap” feature is advertised in their marketing**
- **Zero Click – no nefarious link clicking required!**
- **Can not be used on U.S. phones ...sorta.... (more on this later)**
- **Installation: NSO claims “stealth” OTA, through rigged public WiFi, and usual (emails and texts, actual people)**

# Who is Pegasus?

- **Irony:** Founders are *not* from the Israeli intelligence sector. Shalev Hulio and Omri Lavie, were just techie startup guys looking for a product that worked (NSO stemmed from CommuniTake)
- **NSO partner:** Niv Karmi – former Mossad and Israeli intelligence officer
- **Research team:** Most come from AMAN, the Israeli Military Intelligence Directorate, including Unit 8200 (extremely elite intelligence unit trained specifically in cyberintelligence)
- **Money Backers:** Initially included Circles, an Israeli cyberweapons firm, and U.S. investment firm Francisco Partners; Novalpina (U.K) bought it in 2019 → Gideon Holdings (U.S.) ← [Stay tuned for more on this later](#)
- **Government Backing:** Licenses must be approved by the Israeli Defense Ministry; allegedly,
  - this is meant to function as oversight to prevent its abuse. (Wasn't all that effective, apparently)
- **Ethics committee:** Initially made up of veteran U.S. foreign policy officials to “advise” on potential customers

# Is Pegasus Legal?

- **Executive order signed in March 2023 bans U.S. government from using it**
  - In response to the revelation over 50 U.S. government officials, both overseas and on U.S. soil, were attacked using the spyware
- Prior to that, **U.S. wiretapping laws kinda-sorta prevented (but also sorta allowed)** spyware from being used against U.S. citizens on U.S. soil
  - On one hand, private citizens have **Fourth Amendment protections**
  - On the other hand, Patriot Act Sections 218 and 213
    - **Section 213:** Allows the government search private property without notice to the owner.
    - **Section 218:** Enables collection of foreign intelligence information
  - The Patriot Act is an expansion on **FISA Section 207**, which was already expanded to include literally anything on anyone allegedly relevant to a “criminal investigation”
- *Gets a bit murky when a U.S. citizen is in another country and tangentially or directly involved in an ongoing investigation or has any contact whatsoever apparently with anyone for any reason in a foreign country.*
- **Spyware is still used by the U.S. government secret squirrel agencies in active investigations**
  - Cleopatra Holdings is still paying for the use of Landmark
  - DEA is authorized to use Graphite
  - NSA conducts PRISM and upstream searches literally all. the. time.

# How much does it cost?

## 2016 Price List (the price has likely gone up )

- › Based on number of targets
  - › \$500,000 installation fee
  - › 10 iPhone or Android users: \$650,000
  - › 5 Blackberry users: \$500,000
  - › 5 Symbian users: \$300,000
- + setup fee

**Need to spy on MORE people? Affordable upgrades!**

- 100 extra targets: \$800,000
- 50 extra targets: \$500,000

# How much does it make?

- › Sales doubled starting from tens of millions from the start (to \$60 million by 2014)
- › **U.S. investment firm bought 70 percent of shares for \$130 million**
- › **Those same shares bought back by one of the founders and a U.K. firm (Novalpina) in 2019; Novalpina offloads it into Gideon Holdings (U.S. company)**
- › \$55 million contract signed with Saudi Arabia in 2017 (and that's just *one* contract...there's so. Many. More.)
- › NSO's geolocation tool, Landmark, charges *per query* – and investigations require a lot of queries.

# THE GOOD

## Mexico

- Used to capture **El Chapo (Joaquin Guman Loera)**, major drug lord
- Effectively used in some drug cartel operations

## Europe

- Effectively used to stop several terrorist plots
- Took down a child trafficking ring with participants that spanned 40 countries
- Potentially has stopped a number of mass terrorism attacks
- Amplifies the efficacy of multi-national collaborative efforts

## U.S.A. / Djibouti

U.S. (CIA) allegedly buys Pegasus for Djibouti, a key access point for us in the Middle East in the G.W.O.T.  
**\*\*Djibouti denies purchase & use of this spyware**

Djibouti has a horrendous human rights record. However, it is undeniably strategically critical. #ItsComplicated\*

# THE BAD

## Mexico

- Deployed against journalists and activists, including soda tax proponents
- Used against **Alejandro Encinas**, human rights official investigating military abuses, in **May 2023** (Citizen Lab conducted forensics)

## U.A.E.

- Used it to spy on human rights activist
- Used to spy on associates of journalist Jamal Khashoggi (killed and dismembered in 2018); conflicting forensics on this but we do know for certain Khashoggi's inner circle was directly attacked
- Aggressively targeted women activists

# International Coinkydinks

- **India:** July 2017 Narendra Modi (Hindu nationalist) **reverses decades-long commitment to the Palestinian movement** after buying \$2 billion of intelligence and weapons from Israel, featuring Pegasus
- **Poland:** November 2016 Prime Minister Beata Szydlo visits Israel to buy Pegasus for its “Central Anti-Corruption Bureau.” Shortly after three opposition members were found to have been attacked by Pegasus.
- **Panama** Pres. Ricardo Martinelli, denied surveillance tools by the U.S. in 2009. In 2010, is **one of only six countries to vote against a war crimes investigation against Israel.** One week later, Martinelli visits Israel. Martinelli orders Pegasus be used against basically everyone domestically, including his mistress. **Votes with Israel on pretty much everything.**



Illustrations by [Pixeltrue](#) on [icons8](#)





# International Coinkydinks

- **U.A.E.:** Massad poisoned a senior Hamas individual *within U.A.E. borders*. Israel offers to sell them Pegasus, U.A.E. buys it, **almost immediately every dissenting voice is tapped.**
- **Ahmed Mansoor** \$140,000 stolen from his account, location monitored, email hacked, passport seized, fired, beaten by strangers several times. **In 2018, sentenced to 10 years in prison for FB and Twitter posts.**
- **Must be the Money:**

2018: Khashoggi killed; NSO claims its forensics analysis found no use of Pegasus against Khashoggi; however some evidence exists that his closest inner circle was attacked.

  - NSO ethics committee agrees to cut Saudi Arabia off
  - **2019: Novalpina (U.K. equity firm) and Shalev Hulio, NSO founder, buys shares from when company is valued at \$1B**
  - **2020: U.A.E.'s Pegasus spigot turned back on**



Illustrations by [Pixeltrue](#) on [icons8](#)



# Where Are We Now?

- › **U.S. issues a 2023 March executive order banning cybersurveillance technology use by U.S. Government**
- › FBI confirmed purchasing Pegasus for study, not use in 2022
- › Biden administration blacklisted NSO in 2019; this *has* had an impact on both NSO employees' willingness to work for the company and its customer base. Also killed L3 Harris defense contract. **Israel sees this blacklisting as an act of war.**
- › **Phantom** was designed to ONLY hack U.S. phone numbers and Israel granted a special license to be used for them. All the three-letter agencies were super excited, but ultimately did not buy it.
- › **Landmark** – NSO's geolocation tool, was still getting U.S. Gov't. payments as of April 2023
- › There is a global surveillance industry worth billions. Plenty of **private, commercial software companies** are working with (or as de facto arms of) governments to bypass domestic warrant laws or other civil privacy protections.

# Can't Use Pegasus?

- In-house developed software specifically designed to circumnavigate warrant requirements
- Landmark, NSO Geolocation tool, **unknowingly**

**Just use the off-brand!**

- The NSA has considered using **Phantom**, also made by NSO but granted a special license allowing it to ONLY be used on U.S. numbers.
- The CIA, FBI, DEA, Secret Service and U.S. Africa Command all were interested, too.
  - Ultimately, the U.S. backed out
  - Landmark, NSO geolocation tool, is still getting payments from Gideon Holdings as of April 2023 (U.S. company)



# The same, but different

- DEA **is** allowed to use **Graphite**, made by Paragon, another Israeli company, for drug cartel investigations. **Bonus: Graphite yinks info from the cloud!\*\*\***
- \*\*\* DEA declined to buy Pegasus in 2017 and claims this is NEVER used against U.S. citizens... (in America...?)



# What's Being Done?

- › **The Pegasus Project:** Collaboration of journalists in 10 countries coordinated by Forbidden Stories.
- › **Amnesty International Security Lab:** Confirms targeting and infections on phones
- › **Current investigations into NSO:**
  - France
  - Mexico
  - Poland
  - Spain
  - India
- **EU formed the PEGA Committee:** Investigates use of spyware in Europe
- **Citizen activist collectives** – Protect journalists, inform on privacy techniques

# What's Being Done?

- **Executive order issued March 2023 banning use of Pegasus by U.S. government**
- **U.S. Sanctions (more than a “very angry letter”)**
  - **Specifically, placed on the U.S. Commerce Dept. “Entity List”**
    - Prevents NSO from using Amazon cloud services and Dell computers
    - Has caused many highly skilled technologists to question working for outright leave the company
    - Makes it a bit more dodgy to purchase the software
    - Killed the L3Harris deal



# What's Being Done?

## The WhatsApp Lawsuit (filed in 2019)

Meta claims it can prove a Washington, D.C. phone number has been attacked by Pegasus

Turned out, that was actually a number being used by NSO to demo Phantom to the FBI (whoops).

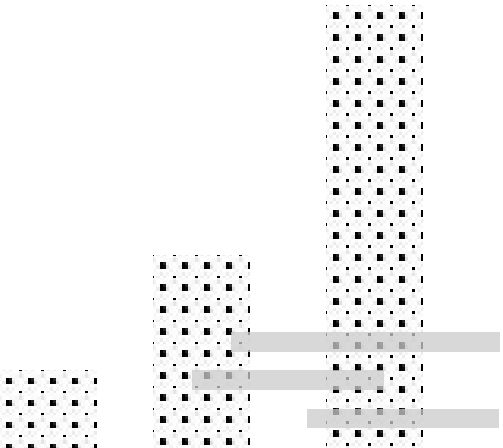
Still, lawsuit alleges 1,400 people were surveilled using WhatsApp

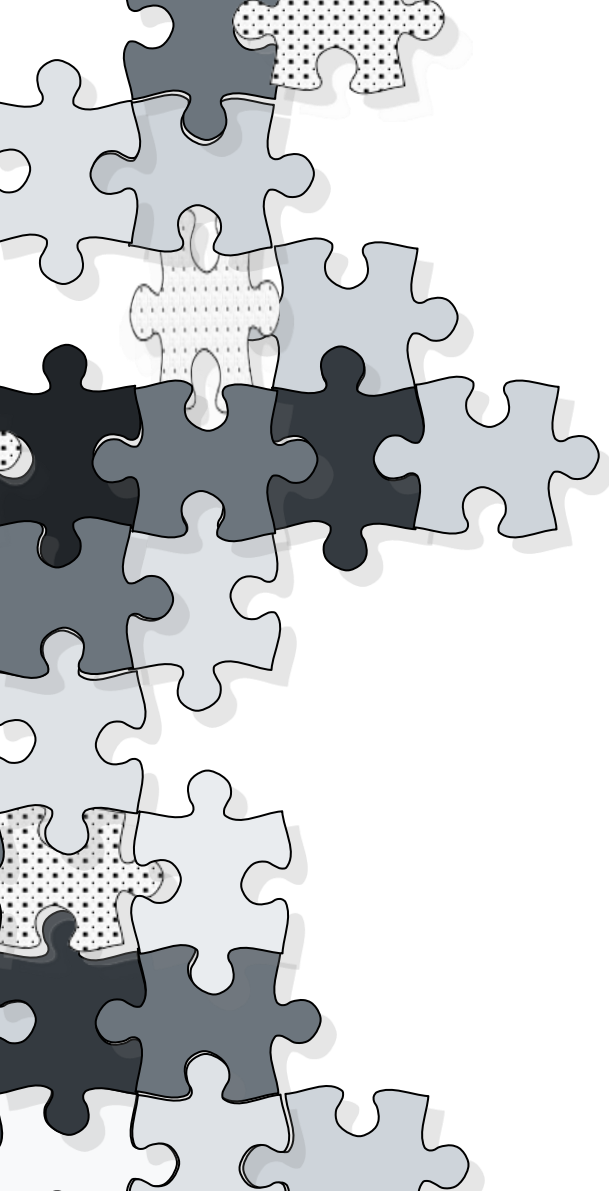
**What they want:** Ban NSO from using its servers, financial damage

## The Apple Lawsuit (filed in 2021)

Alleges Pegasus was used to surveil Apple users

**What they want:** Deletion of previously acquired data; banned from using Apple servers, and money





“ Once NSO systems are sold, governments can essentially use them however they want. **NSO can say they’re trying to make the world a safer place, but they are also making the world a more surveilled place.** ”

Bill Marcsz, Citizen Lab at Munk School of Global Affairs, University of Toronto, quoted in *New York Times*, “How Spy Tech Firms Let Governments See Everything on a Smartphone,” digital publication on 9/2/2016



# References and Further Reading

- *New York Times*, "[The Battle for the World's Most Powerful Cyberweapon](#)," Published Jan. 28, 2022 Updated June 15, 2023
- *Scientific American*, "[What is Pegasus? How Surveillance Spyware Invades Phones](#)," August 9, 2021
- *Wall Street Journal*, "[Biden Restricts Use of Commercial Hacking Tools by U.S. Agencies](#)," March 27, 2023
- *New York Times*, "[How Spy Tech Firms Let Governments See Everything on a Smartphone](#)," digital publication on 9/2/2016
- *Columbia Journalism Review*, "[The Hacker](#)," *The Authoritarianism Issue*
- *New York Times*, "[How Mexico Became the Biggest User of the World's Most Notorious Spy Tool](#)," April 18, 2023
- *Foreign Affairs*, "[The Autocrat in Your iPhone](#)," January/February 2023, by Ronald J. Deibert, founder of Citizen Lab
- *Haaretz*, "[What Did the FBI Really Want NSO's Pegasus For?](#)" Feb. 6, 2022
- *Amnesty.org*, "[The Pegasus Project: One year on, spyware crisis continues after failure to clamp down on surveillance industry](#)," July 18, 2022
- *Council on Foreign Relations, cfr.org*, "[How Israel's Pegasus Spyware Stoked the Surveillance Debate](#)," March 8, 2022



Photo by [Dave Hoefler](#) on [Unsplash](#)



# References and Further Reading

- *New York Times*, "[A Front Company and a Fake Identity: How the U.S. Came to Use Spyware It Was Trying to Kill](#)," April 2, 2023 (updated April 10)
- ACLU Newsletter, "[Five Things to Know About NSA Mass Surveillance and the Coming Fight in Congress](#)," April 11, 2023
- *New York Times*, "[Who Paid for a Mysterious Spy Tool? The F.B.I., an F.B.I. Inquiry Found](#)," July 31, 2023



Photo by [Dave Hoefler](#) on [Unsplash](#)