# The Spyware Market

By Lekhana Molleti (darivxe)

## *Contents*

## 1.1 Executive Summary

This investigation provides a comprehensive analysis of the global commercial spyware ecosystem, encompassing major suppliers, vendors, high-profile scandals, corporate incidents, public disclosures, legal implications, and emerging trends. Spyware, traditionally framed as lawful interception tools for government use, has repeatedly been misused for political, corporate, and personal espionage.

Key findings include:

- **Market Players:** NSO Group, Candiru, Intellexa Alliance, Paragon Solutions, Hacking Team, Gamma Group, Cellebrite, RCS Labs, and Quadream dominate the spyware market, serving both as developers and direct vendors to state clients.

- **High-Profile Misuse:** Investigations such as the Pegasus Project, Predator Files, Reign spyware exposure, and historic Hacking Team/FinFisher leaks reveal that spyware is often deployed against journalists, opposition figures, and human-rights defenders.

- **Corporate Impact:** Corporations are not only targets but also whistleblowers and litigants against spyware misuse, as evidenced by Meta/WhatsApp, Apple, and Amazon/Bezos cases.

- **Public Disclosure and Accountability:** Hacktivists, NGOs, and investigative journalists—including Citizen Lab, Amnesty International, and the Atlantic Council DFRLab—have been instrumental in exposing spyware campaigns, forcing legal and regulatory actions.

- **Legal Landscape:** Revelations about spyware operations have prompted policy responses, including EU PEGA recommendations, U.S. Executive Orders, export control measures, visa restrictions, and major lawsuits establishing vendor accountability.

- **Future Trends:** The spyware market is expected to grow in sophistication and reach, driven by technological advances, geopolitical demand, regulatory gaps, and commercial incentives. Modular, cross-platform, zero-click capable spyware will likely expand market accessibility while leakage and public exposure will inadvertently diffuse capabilities.

## 1.2 Scope of Investigation

This investigation examines the global **spyware ecosystem**, focusing on the structure, operations, and implications of its commercial market. The scope includes identifying **spyware suppliers and vendors**, their **hardware and software offerings**, marketing methods, and global presence. It further investigates **notable spyware scandals**, **corporate incidents**, **public disclosures**, and **legal and regulatory actions** that have shaped the industry. Using **Open Source Intelligence (OSINT)** techniques, this study collects, verifies, and analyzes publicly available data from reports, official documents, and media sources to map key actors, expose market behaviors, and assess the broader impact of spyware on **privacy, governance, and human rights**.

## 1.3 Methodology

The investigation followed a structured OSINT and analytical framework to ensure comprehensive coverage of spyware suppliers, vendors, and their operations.

1. Data Collection:

Open-source intelligence (OSINT) from news media, NGO reports, academic publications, and cybersecurity advisories.

Primary sources included Citizen Lab investigations, Amnesty International Security Lab reports, Atlantic Council DFRLab publications, and official corporate filings or press releases.

Publicly available court documents, export control notices, and Entity List announcements provided legal context.

2. Vendor and Product Analysis:

Identified major spyware suppliers and vendors and documented their marketing approaches, operational models, and product capabilities.

Compiled tables summarizing the target markets, technical capabilities, and high-profile misuse incidents for each vendor.

Traced delivery methods, customer support structures, and event participation to illustrate commercial strategies.

3. Incident Investigation:

Examined historical and recent spyware scandals, including Pegasus, Predator, Reign, Hacking Team, and FinFisher. Focusing on targets, trigger events, spyware delivery, and consequences.

Evaluated corporate incidents where spyware intersected with business operations, including Operation Aurora, Night Dragon, and DarkHotel campaigns.

4. Legal and Policy Review:

Analyzed the impact of spyware revelations on international and domestic legal frameworks, export controls, and corporate governance.

Documented lawsuits, regulatory actions, and executive orders resulting from spyware exposure.

5. Trend Forecasting:

Assessed technological, geopolitical, and market factors influencing the future proliferation and diffusion of spyware.

Incorporated public reporting, threat intelligence analyses, and expert commentary to anticipate emerging patterns in spyware development, deployment, and regulation.

6. Documentation and Presentation:

Findings were systematically organized into sections, supported by tables, charts, and screenshots.

References were meticulously cited to ensure traceability and credibility.

---

## *2.1 Understanding the world of Spyware*

1. What is Spyware?

Spyware refers to software intentionally designed to **monitor, collect, and exfiltrate data from a digital device without the knowledge or consent of the user**. Unlike traditional malware, which typically seeks to disrupt or damage systems, spyware emphasizes **covert surveillance and persistence**. Modern spyware can capture keystrokes, extract messages and call logs, access location data, and remotely activate microphones and cameras.

2. What is the purpose of spyware?

The overarching purpose of spyware is to **enable targeted surveillance and intelligence collection**. The objectives differ according to the actor deploying it:

- **Government and security services –** monitor criminal suspects, terrorists, political opponents, journalists, or civil society groups.
- **Corporate actors –** conduct competitive intelligence or monitor employees.
- **Criminal enterprises –** harvest credentials, financial data, or personally identifiable information for profit.
- **Private individuals –** use of "stalkerware" marketed as parental control software but repurposed for intimate partner surveillance.

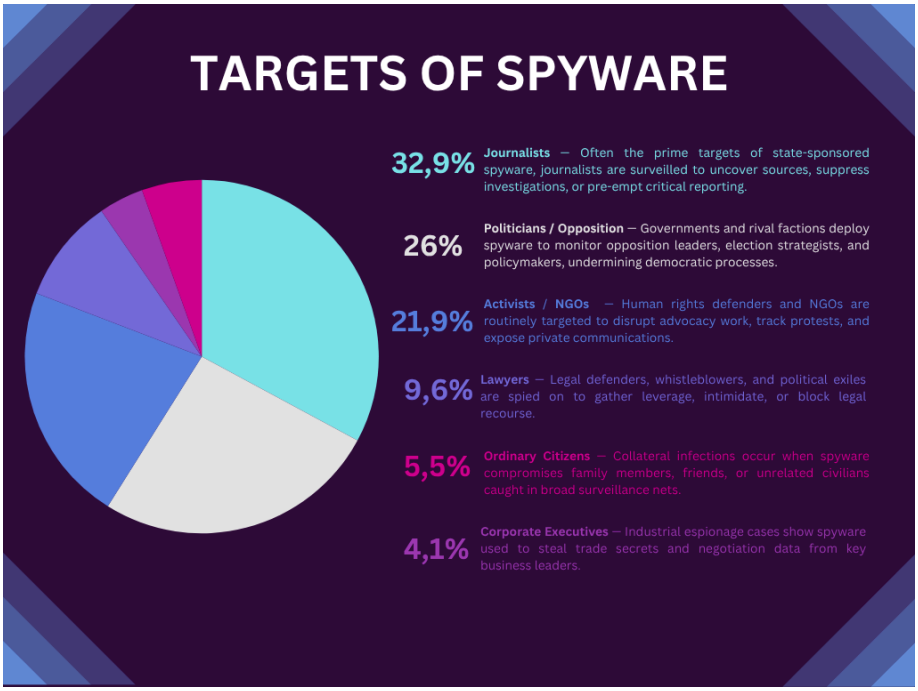
*In all contexts, spyware transforms a device into a* ***sensor for the operator****, providing continuous access to private communications and activities.*


*How Spyware works?*

3. Who uses spyware?

Spyware has been deployed by a wide spectrum of actors:

- **Nation-states –** Numerous governments have procured commercial spyware. For example, Pegasus has been linked to deployments in Mexico, India, and Hungary.
- **Law enforcement agencies –** In 2025, reporting confirmed that U.S. Immigration and Customs Enforcement (ICE) procured *Graphite*, a spyware tool marketed by Paragon.
- **Authoritarian regimes –** Tools such as FinFisher's *FinSpy* have been documented in countries including Egypt, Ethiopia, and Turkey.
- **Private users –** Commercially available stalkerware remains widely accessible through online marketplaces.




4. Who creates and distributes spyware?

The spyware ecosystem is composed of multiple actors:

- **Vendors –** Companies that design, develop, and sell spyware as "lawful intercept solutions" (e.g., NSO Group, Intellexa Consortium, FinFisher GmbH).
- **Subsidiaries and Resellers –** Smaller firms or regional distributors that rebrand and sell products on behalf of larger vendors (e.g., Cytrox under Intellexa).
- **Suppliers and Exploit Brokers –** Entities providing zero-day vulnerabilities, infrastructure, or technical modules integrated into spyware platforms.

- **Investors and Holding Companies –** Financial stakeholders who fund and structure spyware vendors, often shielding them from direct legal liability.

Distribution is typically conducted through **confidential government contracts** and showcased at **cybersecurity and defense trade fairs** under the label of lawful surveillance. However, leaked documents and independent investigations consistently demonstrate that spyware is marketed far beyond its stated purpose of criminal and counter-terrorism investigations.

---

## ~ *History Of Spyware*

### ★ The Appearance of the Word "Spayware" - 1995

On October 16, 1995, Roland Vossen's Usenet post contained the first recorded use of the word '*spyware*'. His post contained about 150 lines of pseudocode mocking Microsoft's release cycles. One of the include statements in the code referenced a file called **spyware.h** *appearance of spyware*

### ★ Bonzi Buddy - late 1990s

Not long after, PCs really did start seeing software that spied or acted in ways users didn't want. By the late 1990s, programs like Bonzi Buddy were riding the wave of Windows popularity. Marketed as a "fun desktop companion," Bonzi's purple gorilla told jokes and helped with browsing but underneath, it tracked user behavior and showed ads. *bonzi-buddy*

### ★ Back Orifice - 1998

Around the same time, hackers released Back Orifice (1998, Cult of the Dead Cow). Unlike Bonzi Buddy's corporate adware vibe, Back Orifice showed how easy it was to remotely monitor and control a Windows machine without consent. It wasn't marketed as spyware, but its *capabilities* such as keylogging, file access and remote control. *Back-Orifice*

### ★ Spyware going commercial - 2000s

Companies like **Gator/Claria** bundled ad software with "free" utilities. Users downloaded what they thought were helpful tools, but hidden processes tracked browsing habits, injected ads, and sent data back. This blurred the line between commerce and intrusion, and sparked lawsuits and FTC attention.

Ordinary users faced pop-up storms and hijacked browsers from families like **CoolWebSearch**. Microsoft and security vendors had to start building anti-spyware definitions because it was everywhere. *Coolwebsearch.H*

★ **Detecting Spyware - 2000s**

By the early 2000s, people were fed up with programs sneaking onto their PCs. That's when security researcher Steve Gibson released **OptOut**, one of the first tools built specifically to detect and block spyware. Once, users had a way to resist. *OptOut*

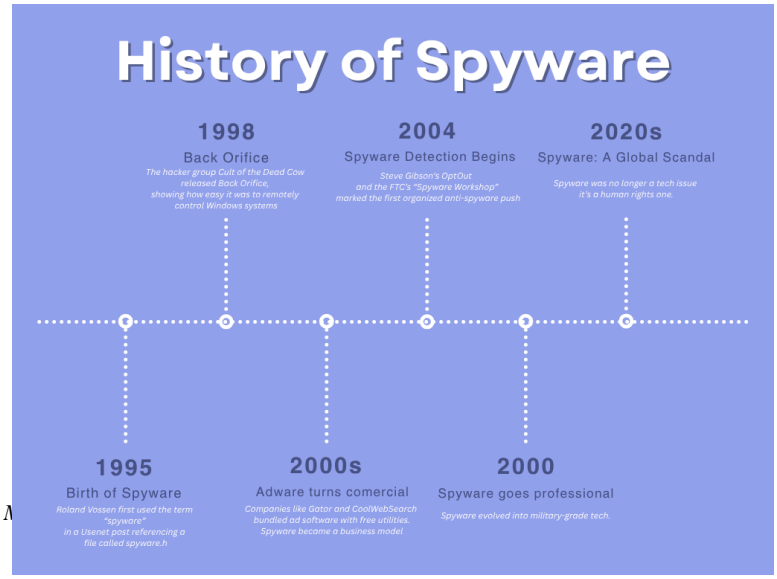
At the same time, regulators started paying attention. The U.S. Federal Trade Commission even held a **"Spyware Workshop"** in 2004, trying to pin down what exactly counted as spyware.

★ **Spyware goes professional 2010s - present**

By the 2010s, spyware had leveled up in a terrifying way. It was no longer just about hijacked browsers or sneaky ad pop-ups — it became a tool of governments and intelligence agencies.

Companies like **NSO Group** in Israel developed **Pegasus**, spyware so advanced it could silently infect a smartphone with a single missed call or text message. Once inside, it could read encrypted chats, track locations, turn on the camera or microphone — all without the user noticing.

Investigations by groups like **Citizen Lab** and **Amnesty International** revealed Pegasus wasn't just used against criminals, as vendors claimed, but also against journalists, activists, and even heads of state. Suddenly, spyware wasn't an inconvenience; it was a geopolitical weapon, capable of silencing dissent and undermining democracy. *TheGuardian Article*




*darivxe ~ The Spyware M*

## *2.2 Spyware Suppliers*

Spyware is more than code; it's a commercial ecosystem. Companies package offensive and defensive capabilities into products, brochure-sell to states and brokers, demo at trade shows, and offer training and support. To understand real-world surveillance abuse you must map the suppliers: what hardware they sell, what software they ship, who they are, how they market, and where proof of sales or demonstration lives.


- ***Hardware supplies sold by the Spyware Suppliers***

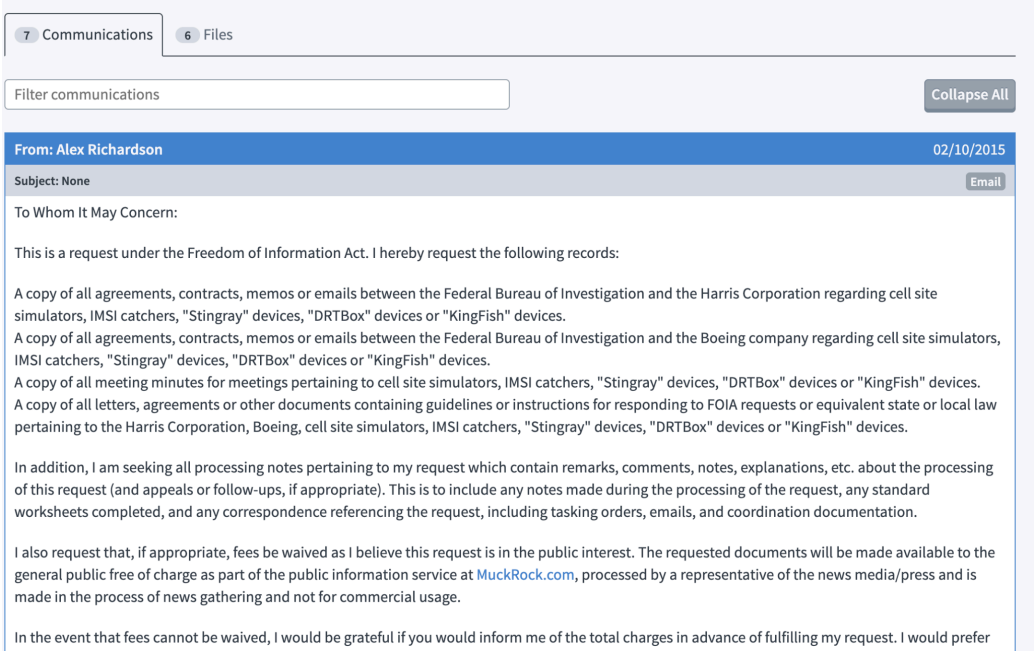
**IMSI-catchers / cell-site simulators -**

**What**: IMSI-catchers, often branded as "StingRay," "KingFish," or similar, are portable devices that mimic legitimate mobile base stations. When activated, they force nearby phones to connect, tricking them into revealing their **IMSI numbers** (International Mobile Subscriber Identity) and other metadata. More advanced models can downgrade encryption (forcing 2G/3G fallback) or even intercept calls and SMS.

**Why**: They are valuable to law enforcement and intelligence agencies for mass location tracking, identifying who is present in a certain area, or targeting a specific person's phone.

But because they indiscriminately scoop up information from all nearby phones, their use raises serious privacy concerns.

***Evidence**: FOIA litigation by the **ACLU** and **MuckRock** forced U.S. agencies to release records of StingRay purchases and NDAs signed with Harris Corporation (the vendor). These documents revealed that agencies had to keep the devices secret, even from courts, highlighting the tension between surveillance secrecy and civil liberties. [MuckRock Evidence]*




*Alex Richardson's request for Stingray Devices*

## Surveillance Vans and Tactical collection kits -

**What**: These are mobile surveillance platforms, often disguised as utility vans, that integrate antennas, IMSI-catchers, radio interception gear, and operator consoles inside a vehicle. They can park near a target area and conduct wireless interception or localized data collection without raising suspicion.

**Why**: Surveillance vans provide "turnkey" tactical collection: everything needed to conduct operations is pre-installed. They allow mobility, discretion, and multi-sensor integration (cellular interception, Wi-Fi sniffing, satellite uplinks).

***Evidence**: Leaked brochures from **Gamma Group's FinFisher** suite (2011) explicitly include references to **"Tactical Surveillance Equipment"** (TSE), including vans outfitted with antennas and racks. These were marketed as part of Gamma's offensive spyware packages. [Gamma FinFisher]*

### Network interception / DPI appliances & lawful-interception racks –

**What**: Deep Packet Inspection (DPI) appliances are high-throughput boxes designed to sit at telecom or ISP chokepoints. They parse traffic in real-time, reconstruct sessions, and extract metadata or content based on keywords, protocols, or user identifiers. Lawful-interception racks are pre-packaged systems installed by telecoms to follow government interception orders.

**Why**: Unlike targeted spyware implants, DPI appliances can surveil at scale. They provide governments with a "dragnet" capability, collecting communications en masse, analyzing traffic patterns, and identifying "persons of interest".

***Evidence**: The **Atlantic Council's report, "Surveillance Technology at the Fair" (2021)**, documents companies showcasing DPI appliances and interception systems at global arms and security fairs. It highlights how these boxes are marketed as "lawful interception" but enable mass surveillance. [Lawful Interception]*

### Mobile forensic extraction hardware (UFED Infield kiosks) –

**What**: These are hardware devices used primarily in law enforcement to extract data from smartphones. The best-known brand is **Cellebrite UFED** (Universal Forensic Extraction Device). They connect via USB or adapters and can bypass phone security to copy messages, call logs, media, app data, and sometimes even deleted files.

**Why**:Though marketed for legitimate investigations, these tools can be misused in authoritarian contexts, seizing devices from journalists, activists, or opposition politicians. Their hardware form (portable briefcase units or kiosks installed in police stations) makes them accessible to a wide range of agencies.

***Evidence**: Amnesty International exposed misuse of Cellebrite kits in Serbia, where authorities reportedly used them against journalists and activists. The controversy forced Cellebrite to suspend operations in that country in early 2025 [Cellebrite Attack]*

### Covert physical implants & field tools –

**What**: Covert implants are surveillance devices disguised as ordinary hardware – USB sticks, network cards, or cables, that secretly deliver spyware, log activity, or siphon off data. They're designed for situations where attackers (or state agents) can gain at least brief physical access to a target's environment, making them the **perfect complement** to remote spyware.

**Why**: These devices represent the "hands-on" side of spyware operations. They're used for **high-value targets** like diplomats, CEOs, or journalists, where remote exploits may fail or be detected. Unlike software implants, these hardware tools can sit undetected for months or years, maintaining persistence and bypassing traditional defenses.

***Evidence**: The **NSA ANT catalog**, leaked in 2013 and reported by Der Spiegel, described a range of spy gadgets including altered USB sticks and network hardware used by the NSA's Tailored Access Operations. These documents provide independent confirmation that covert implants aren't just vendor promises but are actively developed and deployed at state level. [NSA ToolBox]*

- ***Software supplies sold by the Spyware Suppliers***

While hardware like IMSI-catchers grabs headlines for its physical presence, the software side of spyware is where the real power lies. Suppliers package their offensive capabilities into modular suites bundles of exploits, implants, management consoles, and analytics platforms that work together. Each component fills a role: some break into the device, others live inside it, others manage what's stolen, and still others analyze and present the results. Investigative work by Citizen Lab, Amnesty International, and Reuters has shown that vendors like NSO Group, Intellexa (Predator), and Candiru all market these components as part of turnkey solutions for government buyers.

### Exploit delivery & zero-click modules –

**What**: Exploits delivered over messaging apps, email, or network services to gain entry. In the past, spyware required a malicious link (one-click). Now, advanced vendors offer **zero-click exploits**: infection occurs when a target merely receives a message, call, or push notification, with no interaction required.

**Why**: They bypass the user awareness. Even a cautious journalist or politician who never clicks unknown links can be silently compromised.

***Evidence**: **NSO Group's Pegasus** was caught using Apple's **FORCEDENTRY zero-click exploit** through iMessage in 2021. Citizen Lab captured the exploit chain live, and Amnesty International's forensic report confirmed its use against journalists. forced-entry evidence*

### Implant payloads -

**What**: Once the exploit succeeds, an **implant** is installed. This is the spyware agent that lives on the device. It is modular and can be updated remotely.

**Capabilities:**

- Reading SMS, encrypted chats (WhatsApp, Signal, iMessage, Telegram).
- Exfiltrating contact lists, call logs, calendars, and files.
- Activating microphone and camera invisibly.
- Tracking GPS location in real time.

***Evidence**:*

*Amnesty's forensic analysis of Pegasus found implants pulling **WhatsApp, Signal, and iMessage data**, along with audio/video recordings.Pegasus Implants*

*Predator implants discovered by Amnesty in 2023 demonstrated similar behaviors: silently activating microphones and exfiltrating data. Predator scandal*

### Command-and-Control (C2) servers & operator dashboards -

**What** :Spyware needs somewhere to "phone home." This is where **C2 infrastructure** and dashboards come in. C2 servers receive stolen data, push new commands, and update implants. Dashboards allow operators (often government agents) to select targets, assign tasks, and review collected intelligence.

**Why:** These systems are what make spyware usable at scale. Without C2, an implant is just malicious code sitting on a phone.

***Evidence**: Large-scale internet scanning found **over 1,000 Pegasus C2 servers** across 45 countries. Shows governments operate regional C2 clusters to control infected devices. Pegasus ops*

### Persistence & evasion modules –

**What** : Persistence modules ensure implants survive reboots or updates. Evasion modules clean logs, disguise processes, and prevent anti-virus detection.

**Why:** These are what make spyware "stealthy" enough for long-term surveillance. A journalist or activist might never realize they've been hacked.

### Analytics / case management platforms –

**What** : These are like a  final layer, the **back-end intelligence suite**. Once data is exfiltrated, these platforms index, search, and visualize it. They allow investigators to link contacts, build timelines of conversations, and generate intelligence reports.

**Why:** Without analytics, raw spyware data is overwhelming. These platforms turn it into actionable intelligence — and are marketed as the "value add" that makes spyware systems worth millions of dollars to buyers.

***Evidence****:In the* ***Predator Files (2023)****, Amnesty International and partner journalists revealed that the Predator spyware suite (by Intellexa/Cytrox) included a* ***management console*** *that let clients* ***search through harvested phone data*** *and assign new tasks to implants. This confirms that modern spyware vendors sell full analytics/case-management suites alongside implants.*

---

| Category | Description | Function / Purpose |
|---|---|---|
| IMSI-Catchers (StingRay, KingFish) | Fake base stations capturing nearby phone IDs and metadata. | Enables law enforcement tracking but raises mass privacy concerns. |
| Surveillance Vans & Tactical Kits | Mobile vans with antennas, interception consoles, and uplinks. | Provide covert, mobile data interception. |

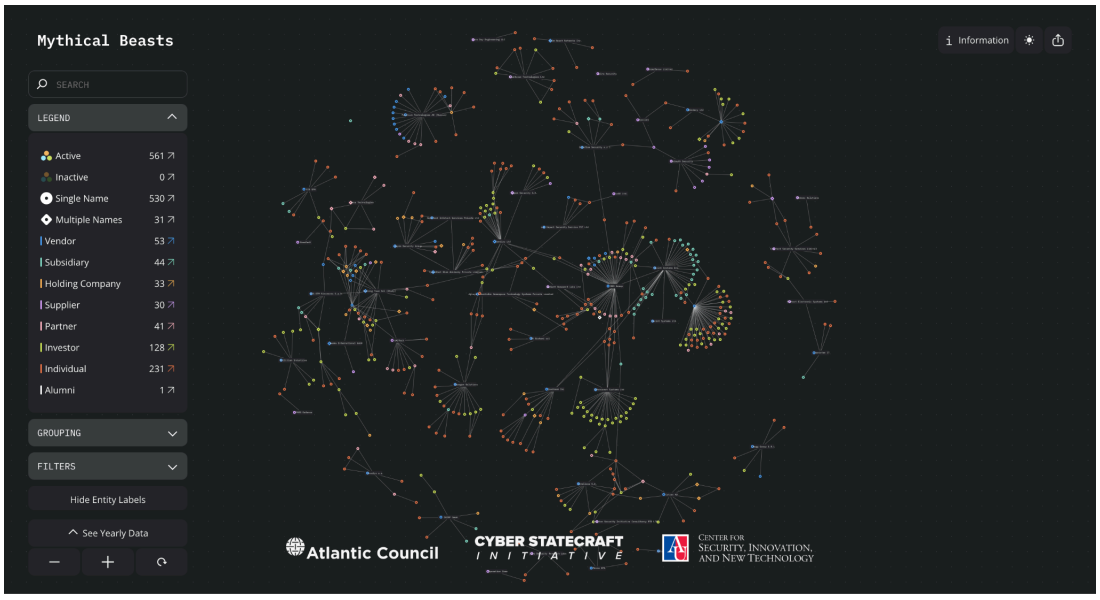
| | | |
|---|---|---|
| Network Interception / DPI Appliances | High-speed ISP-level data filters for packet capture and keyword monitoring. | Facilitates mass network surveillance under “lawful interception.” |
| Forensic Extraction Devices (Cellebrite UFED) | Hardware for smartphone data recovery and bypassing security. | Used legitimately by LEAs but abused in authoritarian contexts. |
| Covert Physical Implants (NSA ANT Catalog) | Modified USB/network hardware that logs or injects spyware. | Used by state-level actors for physical infiltration. |
| Exploit Delivery & Zero-Click Modules | iMessage and WhatsApp exploits enabling remote infections. | Eliminates human error factor in infection. |
| Implant Payloads | Persistent spyware modules harvesting data, media, and chats. | Core surveillance agent for long-term device control. |
| Command & Control Servers / Dashboards | Centralized systems managing infected devices. | Allows scalable government surveillance. |
| Analytics / Case Platforms | Visualization dashboards for collected data and contacts. | Converts raw data into actionable intelligence. |
| Global Supplier Distribution | 435 entities across 42 countries (Israel, EU, US, UAE, Singapore, Cyprus). | Confirms global commercial scale of spyware. |

| | | |
|---|---|---|
| Supplier Marketing Strategies | Marketed as “lawful interception” or “digital intelligence.” | Frames spyware as legitimate tech. |
| Trade Fair Presence | Exhibitions at ISS World, Milipol, Intersec, etc. | Normalizes spyware as a law-enforcement tool. |

---

- ***Suppliers Located Globally***

The *Mythical Beasts* project, published by the Atlantic Council’s Digital Forensic Research Lab (DFRLab), mapped the spyware industry and identified 435 entities across 42 countries that participate in the development, sale, and distribution of spyware technologies. This mapping shows that spyware is not confined to a single region but is part of a global commercial market. *Mythical Beasts Report*




*Mythical Beasts Website*

### *Israel*

- **NSO Group** – Producer of *Pegasus*, one of the most notorious spyware platforms, used against journalists and dissidents worldwide.

- **Candiru (Saito Tech Ltd)** – Developer of commercial spyware used in targeted attacks, sanctioned by the U.S. government.

- **Paragon Solutions (Graphite)** – Emerging spyware vendor; its "Graphite" spyware was reported as used by the Italian government to monitor human rights defenders.

### *Europe*

- **Intellexa Alliance (Greece, Hungary, North Macedonia, and others)** – A consortium that markets the *Predator* spyware. Intellexa is structured across several jurisdictions to obscure ownership and spread operations.

- **Hacking Team (Italy)** – Known for its *Remote Control System (RCS)* spyware, widely sold before the 2015 leaks exposed its global customer base.

### *United Kingdom / Germany*

- **Gamma International / FinFisher** – Producer of *FinSpy*, a spyware suite marketed for "lawful interception," used in multiple countries and documented in past NGO investigations.

### *United States*

- While not traditionally thought of as a spyware exporter in the same way as Israel or Europe, U.S. firms appear in the dataset as **investors and intermediaries**. For example, private equity firms such as **AE Industrial Partners** have invested in Paragon Solutions, illustrating U.S. financial links to the spyware industry.

### *Other Regions*

- **North Macedonia / Hungary** – Producer of *FinSpy*, a spyware suite marketed for "lawful interception," used in multiple countries and documented in past NGO investigations.
- **United Arab Emirates** – Known to have hosted resellers and buyers of spyware solutions, sometimes serving as intermediaries for distribution in the Middle East.
- **Singapore & Cyprus** – Countries flagged in the Mythical Beasts dataset as hosting shell entities or partners linked to spyware distribution.

---

- ***Suppliers Marketing their Products to Vendors***

Spyware is not sold on app stores or open markets — it's marketed quietly, through specialized **channels and narratives**. Suppliers position their products as **"lawful interception tools"** or **"cyber-intelligence platforms"** rather than "spyware".

The Mythical Beasts project shows that suppliers rely on trade fairs, private demos, sales decks, resellers, and careful branding to market their products to government buyers while downplaying risks.

### *Supplier Marketing Approach*

- **NSO Group – *Pegasus***

NSO frames Pegasus as a **lawful interception tool for fighting crime and terrorism**, claiming it is only sold to vetted governments. Marketing language emphasizes "saving lives" and "national security."

NSO public statements and Citizen Lab/Amnesty reporting show Pegasus marketed to governments as an off-the-shelf "turnkey" surveillance solution. The *Citizen Lab "Hide and Seek"* report notes Pegasus's infrastructure patterns correspond to state-level operators, confirming sales to governments. *Pegasus' hide and seek tracking*

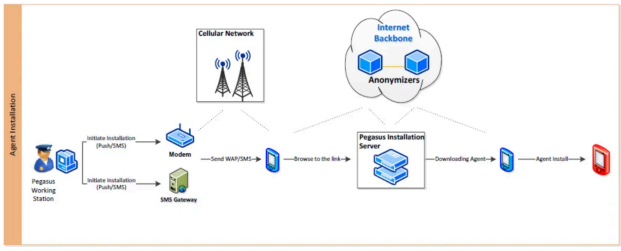



Figure 3: NSO's Exploit Framework [Source: Hacking Team E-mails]

- **Candiru (Saito Tech Ltd)**

Candiru, also known as Devil's Tongue, operated under secrecy but marketed itself as a **specialized spyware vendor** offering modular solutions to governments. Its positioning was similar to NSO's — focusing on "lawful" use cases. Candiru's Infra citizenlab report

| Company name | Date of registration | Possible meaning |
|---|---|---|
| **Saito Tech Ltd.** (סאייטו טק בעיימ) | 2020 | "Saito" is a town in Japan |
| **Taveta Ltd.** (טאבטה בעיימ) | 2019 | "Taveta" is a town in Kenya |
| **Grindavik Solutions Ltd.** (גרינדוויק פתרונות בעיימ) | 2018 | "Grindavik" is a town in Iceland |
| **DF Associates Ltd.** (ד. אף אסוסיאייטס בעיימ) | 2017 | ? |
| **Candiru Ltd.** (קנדירו בעיימ) | 2014 | A parasitic freshwater fish |

**Table 1: Candiru's corporate registrations over time**

A leaked Candiru project proposal published by TheMarker shows that Candiru's spyware can be installed using a number of different vectors, including malicious links, *man-in-the-middle* attacks, and physical attacks. A vector named "*Sherlock*" is also offered, that they claim works on Windows, iOS, and Android. This may be a browser-based zero-click vector.

| Infection Vectors | |
|---|---|
| > Hyperlink | |
| > Weaponized file – Office file OR other (for Windows OS only) | Included |
| > Online physical attack vector (for Windows OS only) | |
| > Dissemination vector between platforms | |
| > Man in The Middle (MiTM) attack vector/price per browser | |
| > Sherlock for Windows, iOS and Android platforms – Optional | (€6,000,000) |
| > Integration to existing tactical solution | |

Figure 2: Infection vectors offered by Candiru.

Like many of its peers, Candiru appears to license its spyware by *number of concurrent infections*, which reflects the number of targets that can be under active surveillance at any one instant in time. Like NSO Group, Candiru also appears to restrict the customer to a set of approved countries.

The €16 million project proposal allows for an unlimited number of spyware infection attempts, but the monitoring of only 10 devices simultaneously. For an additional €1.5M, the customer can purchase the ability to monitor 15 additional devices simultaneously, and to infect devices in a single additional country. For an additional €5.5M, the customer can monitor 25 additional devices simultaneously, and conduct espionage in five more countries.

*Infection Factors offered by Candiru*

- **Paragon Solutions (Graphite, Israel / U.S.)**

Paragon highlights "compliance with democratic values" in its branding, presenting Graphite as a **"next-generation cyber-intelligence" tool**. Its U.S. subsidiary and links to American investors show that it markets itself as a **more "legitimate" alternative** to NSO, after NSO faced global backlash.

The Atlantic Council's *Mythical Beasts: Diving into the Depths* briefly describes Paragon's investor backing and how it was used by Italy, showing active positioning in the European spyware market. *Mythical Beasts report*

- **Intellexa Alliance (Predator - Greece / Hungary)**

Intellexa sells Predator spyware as part of a **broader "cyber-intelligence suite"**. Their sales decks (leaked in media/NGO reports) show claims of advanced device penetration with "lawful use" framing. They also rely heavily on **intermediaries and resellers** to obscure their direct involvement.

The *Amnesty International Predator Files (2023)* report confirms Intellexa marketed Predator to governments, highlighting the management console and analytics capabilities it offered. *The Predator Files markets report*

- **Hacking Team (Italy)**

Hacking Team pitched RCS as a "stealth solution" for law enforcement. They marketed heavily at **international trade fairs** (e.g., ISS World). Their sales materials emphasized how RCS could "go beyond traditional interception" by infecting devices directly.

The 2015 Hacking Team leak exposed internal emails and brochures showing their sales pitches, client lists, and demo screenshots. Wired confirmed they marketed aggressively worldwide. *Hacking Team leak*

- **Gamma International (UK / Germany) - Finfisher**

Gamma marketed FinFisher through **trade fairs and brochures**, branding it as "IT Intrusion" and "lawful interception" software. They pitched FinFisher as a tool for covert, remote surveillance with training included.

The Atlantic Council *Surveillance Technology at the Fair* report shows Gamma appearing at arms/security trade fairs. The FinFisher brochure reveals the marketing language. *Surveillance Technology Report*

- **Cellebrite (Israel) - UFED and Forensic Tools**

Unlike spyware implant vendors, Cellebrite markets its products more openly, positioning UFED devices as law enforcement forensic tools. Marketing emphasizes solving crimes, gathering evidence from suspects' phones, and ensuring "public safety."

Amnesty International reporting showed how Cellebrite marketed to governments worldwide and later restricted some sales after misuse cases (e.g., Serbia in 2025). *Cellebrite report* *Serbia: A Digital Prison*


*Cellebrite's UFED misuse report*

- ***Suppliers at market expos***

Multiple spyware suppliers have been documented exhibiting their products at global cybersecurity and surveillance trade fairs, often under the euphemistic banner of "lawful interception," "digital forensics," or "public safety technologies."
According to the Atlantic Council's Digital Forensic Research Lab (DFRLab) report "Surveillance Technology at the Fair," spyware and interception vendors routinely appear at arms and intelligence expos such as ISS World, Milipol, and Security & Policing (UK) to demonstrate their products to potential state clients.

These expos serve as marketplaces for surveillance technology, connecting suppliers with defense ministries, law enforcement agencies, and private brokers. Vendors use these events to normalize their tools as legitimate law-enforcement technologies.

- **NSO Group**

While NSO does not openly advertise its participation, industry reports and NGO investigations confirm that Pegasus was **pitched to governments through private booths and restricted sessions** at ISS World events. NSO representatives have historically attended under "lawful interception" categories, alongside other Israeli vendors.

- **Candiru**

Candiru, like NSO, markets primarily to state agencies and has been observed participating in trade fairs indirectly through front companies and intermediaries. These events provide them cover to network without directly revealing the spyware brand.

- **Paragon Solutions (Graphite)**

Because Paragon seeks to distinguish itself from NSO's controversial reputation, it has taken a more public marketing route by participating in defense and law-enforcement expos under its "cyber-intelligence" branding. Paragon representatives have been observed networking at European trade shows and promoting Graphite as a "next-generation interception platform."

- **Intellexa Alliance / Predator**

Intellexa, the consortium behind Predator spyware, has **exhibited at Milipol (Paris)** and **Security & Policing (London)**, often under vague descriptions such as *"information analysis platforms"* or *"intelligence support solutions."* These expos allow Intellexa to market Predator without explicitly labeling it spyware.

- **Hacking Team**

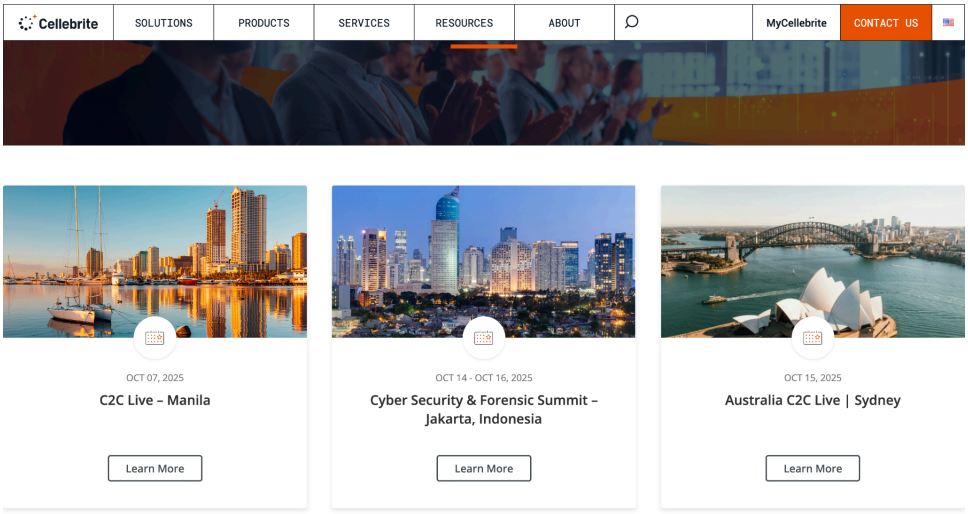
Before its 2015 leak and collapse, Hacking Team was one of the **most active spyware vendors at international expos**. It regularly presented its *Remote Control System (RCS)* at **ISS World**, **Milipol**, and **Security & Policing**. Marketing material described it as "the hacking solution for law enforcement."

- **Gamma Group / Finfisher**

Gamma Group promoted *FinFisher / FinSpy* at arms and surveillance fairs as a **"lawful interception system."** The Atlantic Council report lists Gamma among companies exhibiting at **ISS World, Milipol, and Intersec.** *Gamma-Finfisher*

- **Cellebrite**

Cellebrite regularly participates **openly** at law-enforcement expos, including **ISS World**, **Interpol World**, and **Milipol**, where it markets its UFED and Digital Intelligence Platform tools as digital forensics solutions. Cellebrite's own website lists event participation, and Amnesty International has criticized how such open marketing contrasts with later misuse cases. *Cellebrite Events* *Amnesty Report*




*Cellebrite Upcoming Events*

## *2.3 Spyware Vendors*

The Spyware ecosystem blurs the line between Suppliers and Vendors. In most cases they are the same. The same companies that *develop* and *supply* spyware components (exploits, implants, hardware interfaces, and analytics platforms) also *market, license, and sell* them to end-users, typically government clients. In this sense, every "supplier" functions as a "vendor," responsible not only for production but for commercialization, distribution, and after-sale support.

Unlike conventional software markets, spyware distribution does not follow an open retail model. Instead, it operates through **closed, invitation-only sales channels**, where the vendors directly supply national security or law-enforcement agencies. This dual role allows these entities to control the full life cycle of their products from research and exploitation development to client deployment, technical support, and post-sale maintenance.

The suppliers I previously analyzed — including **NSO Group, Candiru, Intellexa, Paragon Solutions, Gamma Group, and Cellebrite**, are all direct vendors as well. They do not rely on resellers alone; instead, they actively **market and sell** their products to government agencies, military intelligence units, and law enforcement bodies under the branding of *"lawful interception"* or *"digital intelligence."*

However, beyond these well-known suppliers, further investigation revealed **additional vendors** who play a critical role in the global spyware trade but operate with even greater discretion. Two notable examples are **RCS Labs** (Italy), Cytrox and **Quadream** (Israel), both of which epitomize the commercial spyware vendor model, selling intrusion platforms directly to state customers while keeping their operations shrouded in secrecy.

- **RCS Labs - Vendor of Hermit Spyware**

RCS Labs, headquartered in Milan, is an established spyware vendor that markets its surveillance tools to government and intelligence agencies. Its flagship spyware, *Hermit*, was exposed by Google's Threat Analysis Group and Lookout in 2022, revealing its use in **Italy, Kazakhstan, and Syria**.
RCS Labs promotes *Hermit* as a *"lawful access solution"*, but technical analysis confirmed it functions as a full-device spyware suite capable of harvesting messages, contacts, audio, and geolocation data.

The company often works through **telecom intermediaries** to conceal direct involvement and delivers the spyware via SMS and mobile carrier manipulation.

**Product Selling Methods:**

**Direct sales / government contracts:** RCS lists law-enforcement & public-safety clients on its site and sells via direct government channels (export-licensed, closed). Reported use in government anti-corruption and law-enforcement operations implies direct procurement.

**Private demos & closed POCs:** Like other mercenary vendors, RCS uses invite-only demonstrations to vetted clients rather than public sales. (This is standard practice documented across vendor investigations.)

**Telco/technical assistance for delivery:** For Hermit, Google/Lookout reported attackers co-operating with or abusing ISP/carrier capabilities to deliver the implant — RCS's operational model appears to include leveraging local telecom vectors as part of delivery. *lookout article*

| DOMAIN LIST 1 | DOMAIN LIST 2 |
|---|---|
| 119-tim[.]info | milf[.]house |
| 133-tre[.]info | mobdemo[.]info |
| 146-fastweb[.]info | mobilepays[.]info |
| 155-wind[.]info | kena-mobile[.]info |
| 159-windtre[.]info | poste-it[.]info |
| iliad[.]info | rojavanetwork[.]info |
| amex-co[.]info | store-apple[.]info |
| cloud-apple[.]info | wind-h3g[.]info |
| fb-techsupport[.]com | |

*Sample of domains used in Hermit's targeting operations*

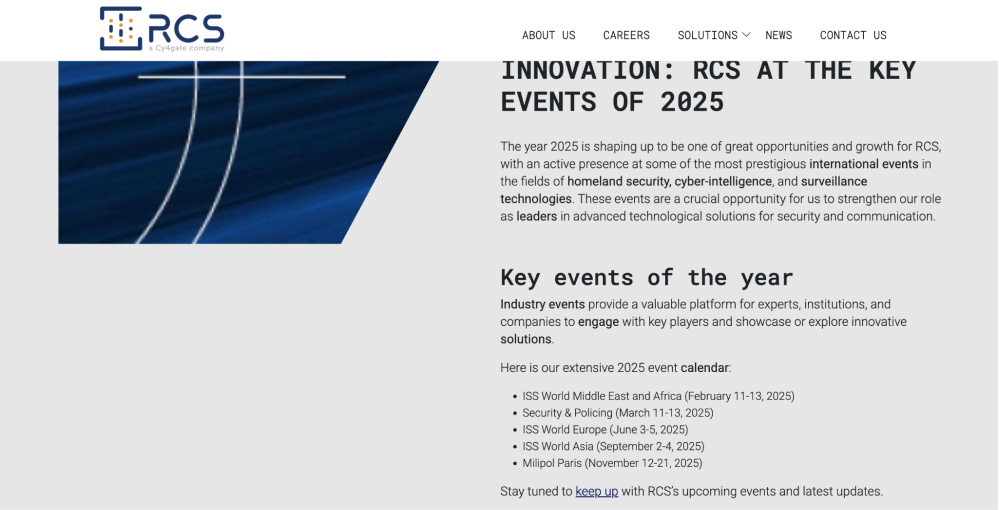
## Customer Support:

**Operational/technical support:** Vendors such as RCS provide installation, integration with client networks, operator training, and ongoing troubleshooting. For Hermit, the technical reports imply vendor involvement in deployment and maintenance (ISP integration, updates).

**Eventual on-site training:** Public reporting about commercial spyware vendors documents typical support tiers: on-site engineers, remote R&D escalation, and update/evade patches *wired article*

### Events and Conferences:

RCS publicly advertises participation at major law-enforcement/expo events (ISS World, Security & Policing, Milipol) on its site and event pages. *rcslab events*




*RCS Labs key events of 2025*

---

- ### QuaDream - Vendor of the *Reign* Spyware

Quadream (also stylized as QuaDream) is an Israeli spyware vendor founded by former NSO Group engineers. The company sold *Reign*, an advanced iPhone exploitation framework capable of zero-click infections similar to Pegasus. Quadream's customers reportedly included governments across the Middle East, Southeast Asia, and Africa.

Operating under extreme secrecy, Quadream conducted its sales through front companies such as *InReach* (based in Cyprus), allowing it to sign contracts while distancing itself from direct vendor liability. Like NSO, Quadream marketed its tools to "trusted law enforcement clients," though forensic analysis by Citizen Lab revealed that its spyware targeted journalists and opposition figures.

## Product Selling Methods:

**Private, brokered sales via shell / intermediary companies:** Reporting shows Quadream used Cypriot/front companies (e.g., InReach) and private brokers to handle contracts to distance the developer from direct public exposure. *citizenlab's article*

> Hackers have been using Israel-developed spyware to target journalists, political opposition figures, and non-government organization workers using iPhones and operating across North America, Central Asia, Southeast Asia, Europe, and the Middle East.
>
> According to two reports published this week by Microsoft and the University of Toronto's Citizen Lab, spyware developed by a relatively obscure Israel-based company, QuaDream, has a significant clientele. This includes the federal governments of Singapore, Saudi Arabia, Mexico, and Ghana. Israel's Haaretz had previously reported that QuaDream sold the spyware to the Saudi government.
>
> Moreover, based on the locations of the servers, the spyware is being operated out of Bulgaria, the Czech Republic, Hungary, Israel, Mexico, Romania, United Arab Emirates (UAE), Uzbekistan, Singapore, and Ghana as well.
>
> https://x.com/jsrailton/status/1645828458235166720?s=20
>
> Microsoft went so far as to refer QuaDream as a private sector offensive actor or PSOA and associated it with a threat group it tracks as DEV-0196. However, a 2022 Reuters report noted that QuaDream doesn't operate the spyware and that its customers are responsible for it, as is the norm.
>
> The QuaDream-developed spyware, marketed as Reign but named KingsPawn by Microsoft, exploits a zero-day vulnerability in iPhones. Dubbed ENDOFDAYS by Citizen Lab, the vulnerability impacts iOS versions 14.4 and 14.4.2 and possibly others.

*Excerpt from Citizen Lab's Quadream Report*

**Invite-only demos / curated client list:** Like other iOS-targeting vendors, Quadream relied on **select, vetted government clients** and did private demos rather than public marketing. *washington-post report*

## Customer Support:

Citizen Lab's investigation shows Quadream provided operators with implants and likely the usual vendor support (on-site/remote assistance, updates to keep exploits working). After exposure, Quadream reportedly shut down operations. *Quadream's exposure*

## Events and Conferences:

**No confirmed public expo booths under the Quadream brand.** Reporting indicates Quadream used intermediaries and private demos rather than exhibiting openly.

> Israeli spyware vendor **QuaDream** is allegedly shutting down its operations in the coming days, less than a week after its hacking toolset was exposed by Citizen Lab and Microsoft.
>
> The development was reported by the Israeli business newspaper Calcalist, citing unnamed sources, adding the company "hasn't been fully active for a while" and that it "has been in a difficult situation for several months."
>
> The company's board of directors are looking to sell off its intellectual property, the report further added.

*TheHackernews Article on QuaDream Shutdown*

---

| Vendor | Product | Country | Sales Model | Client Base | Evidence / Reference |
|---|---|---|---|---|---|
| RCS Labs | Hermit | Italy | Direct contracts & telecom intermediaries | Sold to Italy, Kazakhstan, Syria | *lookout article* *rcslab events* *wired article* |
| QuaDream | Reign | Israel / Cyprus | Brokered through shell companies (InReach) | Sold to ME & African governments | *citizenlab's article* *washington-post report* *Quadream's exposure* |
| NSO Group | Pegasus | Israel | Direct to vetted governments | Used by 40+ countries | *amnesty* |

| | | | | | |
|---|---|---|---|---|---|
| Intellexa Alliance / Cytrox | Predator | EU Consortium | Reseller intermediaries | Greece, Egypt, Armenia | *predator files* |
| Paragon Solutions | Graphite | Israel / US | Compliance-oriented branding | Western-aligned clients | *mythical beasts report* |
| Gamma Group / FinFisher | FinSpy | UK / Germany | State-level licensing | Multiple repressive states | *finfisher report* |
| Cellebrite | UFED | Israel | Open law-enforcement sales | Global police agencies | *Cellebrite report* |

## *2.4 High Profile Scandals involving Spyware*

Over the last decade, the global spyware industry has repeatedly crossed from "lawful interception" into political espionage. Governments that purchased commercial spyware for counter-terrorism or organized-crime investigations have quietly turned it inward—spying on journalists, lawyers, activists, and political rivals.
Major exposures by *Amnesty International*, *Citizen Lab*, *Google TAG*, and investigative outlets such as *Reuters* and *The Guardian* revealed that the same private vendors selling to democratic allies were simultaneously equipping authoritarian regimes.

### The Pegasus Project (NSO Group – Israel)

**Government use:**
Pegasus, developed by **NSO Group**, was licensed to more than forty governments worldwide—including Mexico, India, Morocco, Hungary, and Poland. Independent forensic analysis proved that state agencies used it to monitor journalists, opposition politicians, and human-rights defenders

**Trigger event:**
In 2021, *Forbidden Stories* and *Amnesty International's Security Lab* obtained a leaked dataset of 50 000 phone numbers potentially selected for surveillance. Subsequent forensic work confirmed dozens of infections, igniting the *Pegasus Project*.

**Spyware and delivery:**
Pegasus exploited **zero-click vulnerabilities** in Apple's iMessage (*FORCEDENTRY*) and WhatsApp. Once installed, it granted full device control—microphone, camera, messages, GPS, and keychain access.

**Consequences:**
– Apple filed suit against NSO; U.S. courts allowed portions of Meta/WhatsApp's case to proceed.
– Israel restricted NSO's export licensing.
– Multiple parliaments opened inquiries (e.g., Poland, Hungary).
– The U.S. Commerce Department blacklisted NSO Group and its affiliate Q Cyber Technologies (Nov 2021). *Pegasus Report*

---

### Predator Files (Intellexa Alliance / Cytrox – EU Consortium)

**Government use:**
The *Predator Files* investigation (Amnesty International 2023) revealed that the **Intellexa Alliance**—a network including Intellexa SA, Cytrox, and Thalestris—supplied the *Predator* spyware to governments in Greece, Egypt, Armenia, and elsewhere.

**Trigger event:**
The Greek opposition politician Nikos Androulakis and investigative journalist Thanasis Koukakis were targeted with Predator. Their discoveries triggered national outrage and parliamentary probes.

**Spyware and delivery:**
Predator relied on **malicious URLs** disguised as news or verification links. Clicking the link silently installed implants through a chain of web exploits.

**Consequences:**
– Resignation of Greece's national-intelligence chief and the prime minister's chief of staff

(Aug 2022).
– EU Parliament hearings on spyware abuse (PEGA Committee).
– The U.S. Commerce Department placed Intellexa entities on the Entity List (2023). *Predator Files*

---

## Reign Spyware (QuaDream – Israel)

**Government use:**
QuaDream—founded by former NSO engineers—sold **Reign**, an iPhone exploit suite, to several Middle Eastern and African governments. Citizen Lab's 2023 analysis found identical forensic artifacts to Pegasus infections.

**Trigger event:**
Apple's threat-notification program warned users of potential state-sponsored attacks. Device forensics later traced infections to QuaDream infrastructure.

**Spyware and delivery:**
Reign exploited **zero-click iMessage vulnerabilities**, requiring no user action. Once inside, it created a temporary file system in RAM to evade detection.

**Consequences:**
– Reuters exposé (Apr 2023) prompted Apple to revoke certificates tied to QuaDream.
– The company reportedly shut down operations months later.

*reign attack on iphones*

---

## Historic Leaks – Hacking Team & FinFisher

**Government use:**
Long before Pegasus, two European vendors pioneered the spyware trade. **Hacking Team** (Italy) marketed its *Remote Control System – RCS* to police and intelligence agencies worldwide; **Gamma International** (UK/Germany) sold *FinFisher / FinSpy*.

**Trigger event:**
In 2015, 400 GB of Hacking Team emails and sales records leaked to WikiLeaks, exposing clients in Sudan, Ethiopia, and Saudi Arabia despite EU sanctions.

**Spyware and delivery:**
Spear-phishing attachments and exploit kits that allowed remote device control.

**Consequences:**
– Immediate reputational collapse; Italy revoked export licenses.
– FinFisher faced German police raids (2019).
– The leaks became foundational case studies for later regulatory reforms.

*wired hackingteam gamma-finfisher*

---

### Project Raven / DarkMatter (UAE – U.S. contractors)

**Government use:**
The United Arab Emirates employed a covert program called Project Raven, run by the private cyber-intelligence firm DarkMatter, to spy on journalists, diplomats, foreign leaders, and even U.S. citizens. The project hired former U.S. NSA and military hackers who used state-grade exploits to monitor targets abroad.

**Trigger Event:**
After internal whistle-blowing and reporting by *Reuters*, several ex-employees exposed how the team, originally contracted for counter-terrorism, shifted to surveilling critics of the Emirati monarchy and Western journalists.

**Spyware and delivery:**
The team deployed an iOS exploitation platform known as Karma, capable of compromising iPhones remotely through Apple's iMessage service, a *zero-click* exploit requiring no user interaction. Once infected, Karma provided access to photos, emails, and location data.

**Consequences:**
- In 2021, the U.S. Department of Justice fined and banned three former NSA contractors for providing hacking services to a foreign government.
- The case became the first major criminal precedent against mercenary spyware operations.
- DarkMatter was dissolved shortly after international backlash.

*Reuters Report*


*Project Raven*

---

## Mexico Pegasus Scandal

**Government use:**
Mexico became NSO Group's largest client, with contracts exceeding USD 60 million. Government security agencies deployed Pegasus against journalists, lawyers, opposition politicians, and even the widow of slain reporter Javier Valdez.

**Trigger Event:**
The campaign came to light when investigative journalists and NGO staff received suspicious text messages linking to fake news pages. Citizen Lab confirmed the links matched NSO's Pegasus infrastructure.

**Spyware and delivery:**
*One-click* SMS and WhatsApp phishing links tricked victims into installing the Pegasus payload. Once compromised, devices were fully accessible to the attacker.

**Consequences:**
- Public outrage forced then-President Enrique Peña Nieto to order an inquiry.
- Under President López Obrador, authorities confirmed ongoing Pegasus use by the military and launched new oversight proposals.
- Pegasus became synonymous in Mexico with domestic espionage scandals.

*reckless exploit*

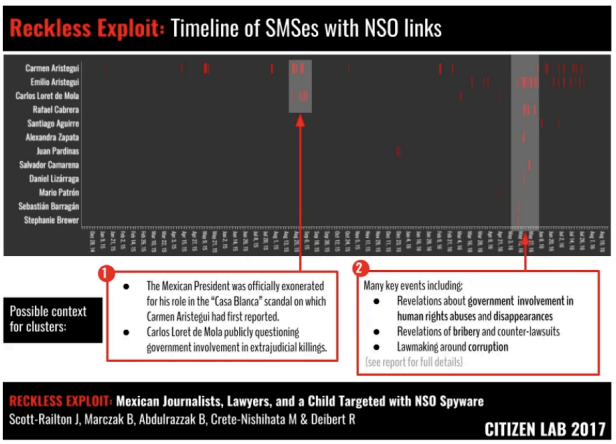



**Figure 2: Timeline of receipt of SMSes with NSO Exploit Links**


**Figure 1: Selected Mexican NSO Targets in media, human rights and anti corruption advocacy, and public health.**

*Mexico-Pegasus Incident - Citizen Lab 2017*

---

## India Pegasus Controversy

**Government use:**
In 2021, revelations from the *Pegasus Project* showed that hundreds of Indian journalists, opposition leaders, and activists were potential targets of Pegasus spyware. Independent forensic tests confirmed multiple infections.

**Trigger Event:**
Phone numbers of senior political strategists, election consultants, and investigative reporters appeared in leaked data analyzed by *Amnesty International* and *The Guardian*. The findings ignited a national debate on surveillance ethics.

**Spyware and delivery:**
Pegasus delivered via zero-click *iMessage* and *WhatsApp* exploits, exploiting unpatched vulnerabilities to gain complete access to iOS and Android devices.

**Consequences:**
– India's Supreme Court ordered a **judicial technical committee** to investigate state spyware use.

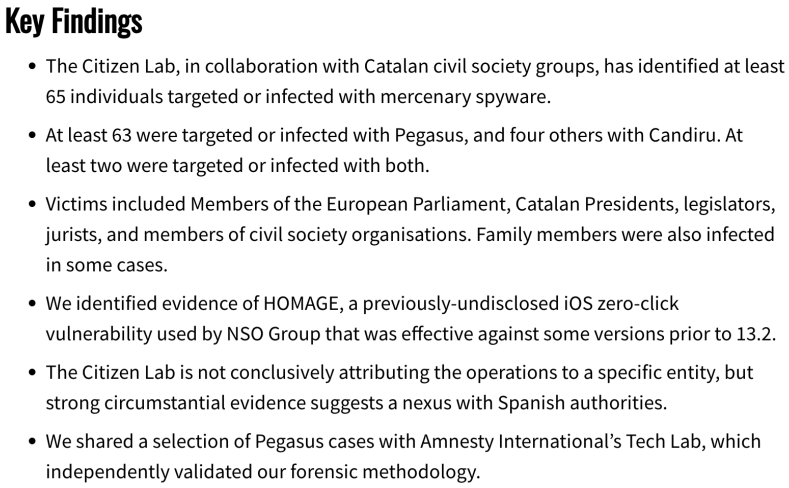
– The government denied wrongdoing but refused to disclose contracts with NSO.
– The case remains a cornerstone example of spyware's use in democratic states.

---

## CatalanGate (Spain – Pegasus and Candiru)

**Government use:**
Spain's National Intelligence Centre (CNI) deployed Pegasus and Candiru spyware against Catalan independence leaders, members of the European Parliament, and NGO staff.

**Trigger Event:**
Citizen Lab's 2022 investigation uncovered 65 infected devices belonging to Catalan politicians, journalists, and lawyers. The Spanish government admitted Pegasus use under court authorization but denied targeting most victims.



### Key Findings

- The Citizen Lab, in collaboration with Catalan civil society groups, has identified at least 65 individuals targeted or infected with mercenary spyware.
- At least 63 were targeted or infected with Pegasus, and four others with Candiru. At least two were targeted or infected with both.
- Victims included Members of the European Parliament, Catalan Presidents, legislators, jurists, and members of civil society organisations. Family members were also infected in some cases.
- We identified evidence of HOMAGE, a previously-undisclosed iOS zero-click vulnerability used by NSO Group that was effective against some versions prior to 13.2.
- The Citizen Lab is not conclusively attributing the operations to a specific entity, but strong circumstantial evidence suggests a nexus with Spanish authorities.
- We shared a selection of Pegasus cases with Amnesty International's Tech Lab, which independently validated our forensic methodology.

**Spyware and delivery:**
Zero-click exploits through *iMessage* and *WhatsApp* injected implants that exfiltrated encrypted chats and documents.

**Consequences:**
– Spain's intelligence chief was dismissed.
– EU Parliament's PEGA Committee opened hearings on member-state spyware misuse.
– "CatalanGate" became the largest documented espionage campaign inside the EU.

*catalangate report*

---

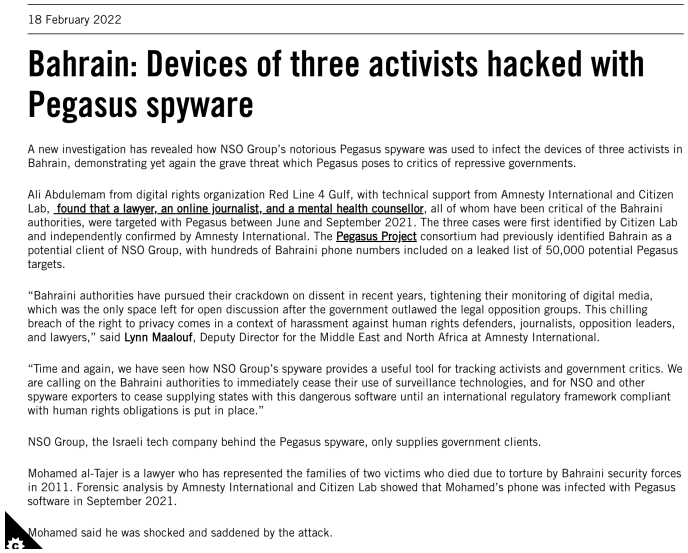
## Bahrain Pegasus Abuse

**Government use:**
Bahrain's authorities used Pegasus to surveil lawyers, opposition figures, and human-rights activists

**Trigger Event:**
After Apple's 2021 security notifications, Amnesty International and Citizen Lab confirmed that several Bahraini activists' iPhones were infected using NSO exploits.

**Spyware and delivery:**
Zero-click *iMessage* and FaceTime vulnerabilities delivered Pegasus payloads enabling microphone and camera control.

**Consequences:**
– Renewed debate on Israeli export licensing for spyware to Gulf states.
– International condemnation and calls for investigation from Human Rights Watch and UN rapporteurs.
*Amnesty Article*



18 February 2022

**Bahrain: Devices of three activists hacked with Pegasus spyware**

A new investigation has revealed how NSO Group's notorious Pegasus spyware was used to infect the devices of three activists in Bahrain, demonstrating yet again the grave threat which Pegasus poses to critics of repressive governments.

Ali Abdulemam from digital rights organization Red Line 4 Gulf, with technical support from Amnesty International and Citizen Lab, found that a lawyer, an online journalist, and a mental health counsellor, all of whom have been critical of the Bahraini authorities, were targeted with Pegasus between June and September 2021. The three cases were first identified by Citizen Lab and independently confirmed by Amnesty International. The Pegasus Project consortium had previously identified Bahrain as a potential client of NSO Group, with hundreds of Bahraini phone numbers included on a leaked list of 50,000 potential Pegasus targets.

"Bahraini authorities have pursued their crackdown on dissent in recent years, tightening their monitoring of digital media, which was the only space left for open discussion after the government outlawed the legal opposition groups. This chilling breach of the right to privacy comes in a context of harassment against human rights defenders, journalists, opposition leaders, and lawyers," said **Lynn Maalouf**, Deputy Director for the Middle East and North Africa at Amnesty International.

"Time and again, we have seen how NSO Group's spyware provides a useful tool for tracking activists and government critics. We are calling on the Bahraini authorities to immediately cease their use of surveillance technologies, and for NSO and other spyware exporters to cease supplying states with this dangerous software until an international regulatory framework compliant with human rights obligations is put in place."

NSO Group, the Israeli tech company behind the Pegasus spyware, only supplies government clients.

Mohamed al-Tajer is a lawyer who has represented the families of two victims who died due to torture by Bahraini security forces in 2011. Forensic analysis by Amnesty International and Citizen Lab showed that Mohamed's phone was infected with Pegasus software in September 2021.

Mohamed said he was shocked and saddened by the attack.

*Amnesty's Article on Bahrain-Pegasus incident*

---

### Ethiopia FinSpy Operations

**Government use:**
Ethiopia's Information Network Security Agency (INSA) utilized FinFisher's FinSpy to monitor exiled journalists and opposition groups

**Trigger Event:**
Citizen Lab identified malicious Word documents sent to diaspora media staff; embedded macros connected to command-and-control servers operated within Ethiopia's telecom network.

**Spyware and delivery:**
Spear-phishing emails carrying booby-trapped attachments exploited Microsoft Word vulnerabilities to install FinSpy modules for keylogging and screen capture.

**Consequences:**
– International pressure on Gamma Group (UK/Germany) for export violations.
– FinFisher raided by German authorities (2019); EU tightened dual-use technology controls. *Finfisher in Egypt*

---

| Case / Year | Vendor / Spyware | Countries Involved | Trigger Event | Key Outcome | Evidence Link |
|---|---|---|---|---|---|
| Pegasus Project (2021) | NSO Group – Pegasus | 40+ govts incl. India, Mexico, Poland | Leak of 50,000 targets via Amnesty & Forbidden Stories | NSO blacklisted; Apple lawsuit; global inquiries | *Pegasus Report* |
| Predator Files (2023) | Intellexa / Cytrox – Predator | Greece, Egypt, Armenia | Greek opposition & journalist hacks | EU & U.S. sanctions | *Predator Files* |

| | | | | | |
|---|---|---|---|---|---|
| Reign (2023) | QuaDream – Reign | Middle East, Africa | Apple alerts linked to QuaDream infra | Apple revoked certificates; firm shut down | *reign attack on iphones* |
| Hacking Team Leak (2015) | Hacking Team / FinFisher | Global (Sudan, Ethiopia, Saudi) | 400 GB internal leak to WikiLeaks | Licenses revoked; FinFisher raided | *wired hackingteam* |
| Project Raven (2019) | DarkMatter – Karma | UAE | Whistleblower reports via Reuters | Ex-NSA hackers fined; DarkMatter dissolved | *Reuters Report* |
| Mexico Pegasus (2017) | NSO Group – Pegasus | Mexico | Citizen Lab exposed fake SMS links | National inquiry; ongoing Pegasus use | *reckless exploit* |
| India Pegasus (2021) | NSO Group – Pegasus | India | Pegasus Project leak names Indian targets | Supreme Court probe; govt denial | *Amnesty* |
| CatalanGate (2022) | NSO / Candiru | Spain | Citizen Lab found 65 infections | Intel chief fired; EU PEGA inquiry | *catalangate report* |
| Bahrain Pegasus (2021) | NSO Group – Pegasus | Bahrain | Apple security alerts & Amnesty findings | Global outcry; export scrutiny | *Amnesty Article* |

| | | | | | |
|---|---|---|---|---|---|
| Ethiopia FinSpy (2019) | Gamma Group – FinSpy | Ethiopia | Malicious docs sent to journalists | FinFisher raided; export violation probe | *Finfisher in Egypt* |

---

## *2.5 Corporate Incidents involving Spyware*

While government espionage dominates most spyware discussions, corporations have increasingly found themselves both **targets and witnesses** of the same surveillance technology.
Commercial spyware now intersects the corporate landscape in several ways. Tech companies have issued **formal statements** about attacks on their infrastructure; executives have been **personally targeted** through sophisticated implants; and threat actors have used spyware as a tool for **market leverage and corporate espionage**.
In parallel, legal and ethical debates have emerged around whether **insiders or whistleblowers** can legitimately deploy monitoring software to expose wrongdoing.

### Corporation Issued Formal Statements

Major tech companies and affected corporations have publicly issued statements, alerts, and lawsuits when spyware abused their platforms or when their executives were targeted.

**Meta / WhatsApp vs NSO (2019–2025):**

WhatsApp (Meta) publicly accused NSO Group of using a WhatsApp vulnerability to install Pegasus on users' phones and brought a lawsuit. The litigation culminated in a 2025 jury decision awarding damages to WhatsApp/Meta. Meta/WhatsApp and their legal filings include public statements and technical analysis. *case overview* *summary judgement*

Case 4:19-cv-07123-PJH Document 494 Filed 12/20/24 Page 1 of 16

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC., et al.,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED, et al.,

Defendants.

Case No. 19-cv-07123-PJH

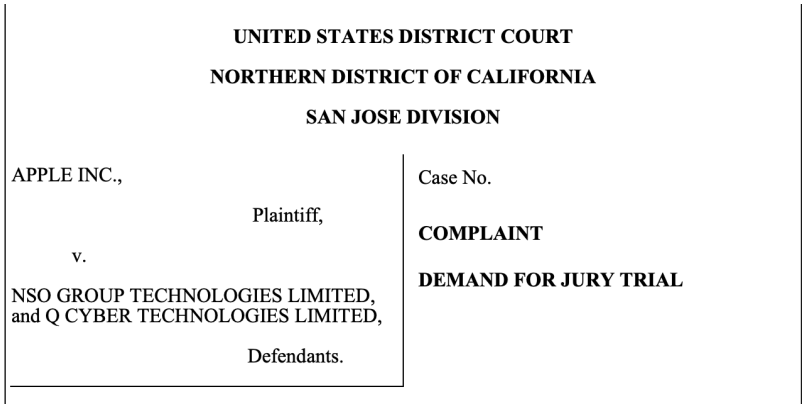
**ORDER RE MOTIONS FOR SUMMARY JUDGMENT, MOTION FOR SANCTIONS, AND DISCOVERY LETTER BRIEFS**

Re: Dkt. 381, 383, 387, 397, 401, 406, 408, 409, 411

*Whatsapp vs NSO Group*


## Apple vs NSO (2021):

Apple publicly sued NSO Group in November 2021; Apple issued a press release and complaint alleging NSO exploited Apple services to target users and sought an injunction. Apple's newsroom and the complaint are official corporate statements about suspected spyware abuse. *apple-news* *complaint doc*



UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

APPLE INC.,

Plaintiff,

v.

NSO GROUP TECHNOLOGIES LIMITED, and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No.

**COMPLAINT**

**DEMAND FOR JURY TRIAL**

*Apple vs NSO formal Statement Excerpt*

### Amazon / Jeff Bezos case (2018–2020):

Jeff Bezos and Amazon publicly discussed allegations of his phone being compromised via a WhatsApp message from Saudi Crown Prince Mohammed bin Salman. Bezos commissioned a forensic analysis (FTI Consulting), and major outlets (The Guardian, Wired, Vice) reported on the findings. *FTI report*

---

## Companies targeted to gain Market Leverage using Spyware

Corporate espionage through spyware has become a persistent threat across global industries, particularly in **energy, technology, and defense**. In these cases, attackers leveraged spyware or spyware-like implants to **obtain negotiation advantages, trade secrets, or intellectual property**.

### DarkHotel Campaign (2014–Present):

The *DarkHotel* Advanced Persistent Threat (APT) campaign, specifically targeted **executives and corporate negotiators** staying at luxury hotels across Asia. The attackers infiltrated hotel Wi-Fi networks, deploying spyware and keyloggers onto guest laptops to harvest credentials, trade secrets, and corporate deal documents. Victims included executives from the defense, energy, and pharmaceutical industries.

This operation represents a classic case of **economic espionage**, where spyware was used for market leverage by stealing confidential information before contract negotiations. *securelist report*

### Operation Aurora (2009):

In a 2009 incident later dubbed *Operation Aurora*, **Google**, **Adobe**, and over 20 U.S. companies were compromised by a cyber-espionage group believed to be operating from China. Attackers exploited Internet Explorer vulnerabilities to install spyware and steal source code and confidential emails.

**Google formally disclosed the incident in a public blog post**, citing "a highly sophisticated and targeted attack" aimed at accessing corporate intellectual property — an early example of a corporation openly identifying spyware as a **market-leverage threat**. *google blog*

### Night Dragon Campaign (2011):

McAfee researchers uncovered Night Dragon, a series of targeted intrusions against Western oil, gas, and petrochemical companies. The attackers used spyware to extract internal emails, pricing data, and negotiation strategies from corporate networks. The campaign's goal was clear: **to provide economic and bidding advantages** to competitors backed by state-linked entities. mcafee report

---

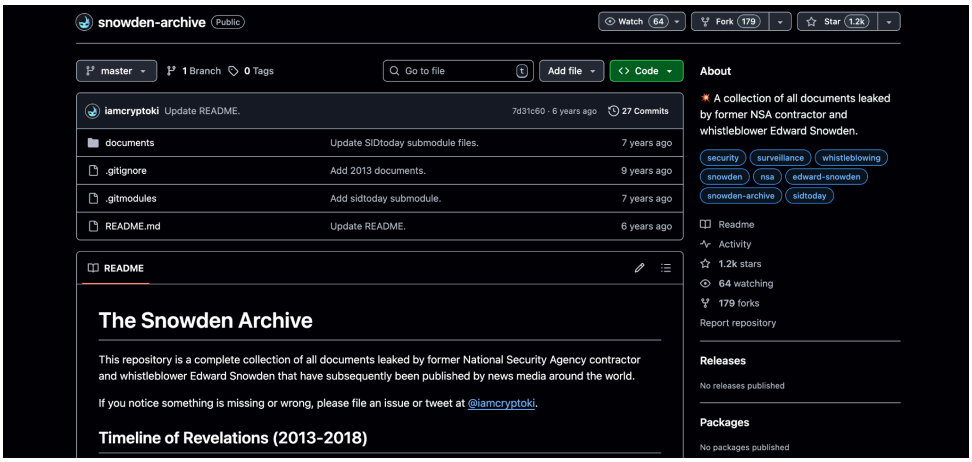
### Employee Use of Spyware for Whistleblowing

While insider leaks and whistleblowing are common in corporate environments, there are **no verified public cases** where an employee deliberately installed commercial spyware as part of whistleblowing activity. Instead, whistleblowers typically use **authorized access** to copy or expose internal data.

### Case Context:

High-profile corporate whistleblowers such as **Edward Snowden (NSA contractor)** and **Frances Haugen (Facebook/Meta)** relied on direct data extraction from systems they had legitimate access to, not spyware. Snowden used administrative credentials to exfiltrate

classified documents, while Haugen collected internal reports and memos to provide evidence to regulators. Neither case involved covert spyware installation or remote surveillance implants. *Snowden article*




*Repository of classified materials released through Edward Snowden's NSA leaks*

### Corporate Policies and Ethical Boundaries:

Most whistleblowing cases fall under **protected disclosure laws**, not espionage statutes. Deploying spyware within a corporation, even for evidence-gathering would violate **data protection regulations (e.g., GDPR, CCPA)** and corporate IT ethics policies. Therefore, employees generally rely on legal whistleblower frameworks or third-party journalists to expose misconduct.

---

## Companies as Victims of Spyware and Corporate Espionage

Apart from previously covered information on companies that have been victims such as Operation Aurora or the NightDragon Campaign, the **Cellebrite Forensic Device Abuse** in (2020–2022) surfaced of law-enforcement-grade spyware and forensic extraction tools (notably **Cellebrite UFED**) being repurposed for unauthorized data access within corporate or private investigations. While not a direct corporate espionage campaign, it illustrates how spyware-grade tools can transition into the private sector and be abused for information theft. *cellebrite-serbia*

Corporations face spyware not only as a platform risk (Apple, Meta) but as **direct espionage targets**. As technology and market competition globalize, the same tools designed for national security are now weaponized against private-sector interests — erasing the boundary between cyberwarfare and corporate warfare.

| Case | Target | Spyware / Attack Type | Motivation / Context | Impact | Evidence / Reference |
|---|---|---|---|---|---|
| WhatsApp vs NSO | Meta / WhatsApp | Pegasus via app call exploit | Platform abuse | Legal victory, damages awarded | *summary judgement* |
| Apple vs NSO | Apple | FORCEDENTRY zero-click | Vendor liability | Lawsuit under CFAA | *complaint doc* |
| Bezos Phone Hack | Amazon (CEO) | WhatsApp payload | Personal espionage | Diplomatic fallout | *FTI report* |
| DarkHotel | Executives in Asia | Wi-Fi-based spyware | Economic espionage | Credential theft, trade data loss | *securelist report* |
| Operation Aurora | Google, Adobe | IE exploit spyware | IP theft | Corporate disclosure, reforms | *google blog* |
| Night Dragon | Oil & Gas firms | Targeted spyware | Market leverage | Bidding advantage to competitors | mcafee report |

| | | | | | |
|---|---|---|---|---|---|
| Cellebrite Abuse | Corporate data extraction | Misuse of UFED kits | Unauthorized access | Product suspension in Serbia | *cellebrite-serbia* |
| Whistleblowing (Snowden) | NSA | Insider data access | Exposure, not spyware | Legal reform wave | *Snowden article* |

---

## *2.6 Public Disclosures as Spyware*

Public disclosure represents the **final stage in the life cycle of spyware**, the point at which covert surveillance operations are forced into public view.
In recent years, the most significant revelations have not come from the corporations that created these tools, but from **hacktivists, investigative journalists, and independent researchers** who uncovered and publicized their inner workings. Through leaks, data dumps, and forensic investigations, these actors have turned the tools of secrecy into instruments of accountability.

### Hacker Groups Using Spyware for Public Data Collection

#### APT28 (Fancy Bear) – Credential-Stealing Implants

The Russian-linked group **APT28**, also known as *Fancy Bear*, used customized spyware and credential-harvesting implants to compromise journalists, NGOs, and election infrastructure worldwide. While its primary goal was political influence, much of the data collected — including voter information and campaign emails — was effectively *publicized* through leaks later used in disinformation operations.

Although this wasn't "commercial spyware," the group used advanced surveillance implants (e.g., **X-Agent**, **Sednit**) that functioned as state-grade spyware. *APT28 Operations*

#### APT38 Lazarus Group (North Korea) – Surveillance via Trojanized Apps

The **Lazarus Group**, tied to North Korea, used spyware-laced cryptocurrency apps to monitor users and steal assets. While primarily motivated by financial gain, the malware also harvested massive

amounts of personal data from victims worldwide which later surfaced in darknet markets and Telegram channels. *Treasury Sanctions*

PRESS RELEASES

## Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups

September 13, 2019

WASHINGTON – Today, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) announced sanctions targeting three North Korean state-sponsored malicious cyber groups responsible for North Korea's malicious cyber activity on critical infrastructure. Today's actions identify North Korean hacking groups commonly known within the global cyber security private industry as "Lazarus Group," "Bluenoroff," and "Andariel" as agencies, instrumentalities, or controlled entities of the Government of North Korea pursuant to Executive Order (E.O.) 13722, based on their relationship to the Reconnaissance General Bureau (RGB). Lazarus Group, Bluenoroff, and Andariel are controlled by the U.S.- and United Nations (UN)-designated RGB, which is North Korea's primary intelligence bureau.

*While hacker groups like APT28 and Lazarus aren't traditional spyware vendors, they effectively weaponized spyware-like implants to exfiltrate data from the public. Their use of data dumps and leaks created de facto "public disclosures" through indirect means — mass data exposure and media dissemination.*

---

### Spyware Used to Gather Information and Publicly Leaked

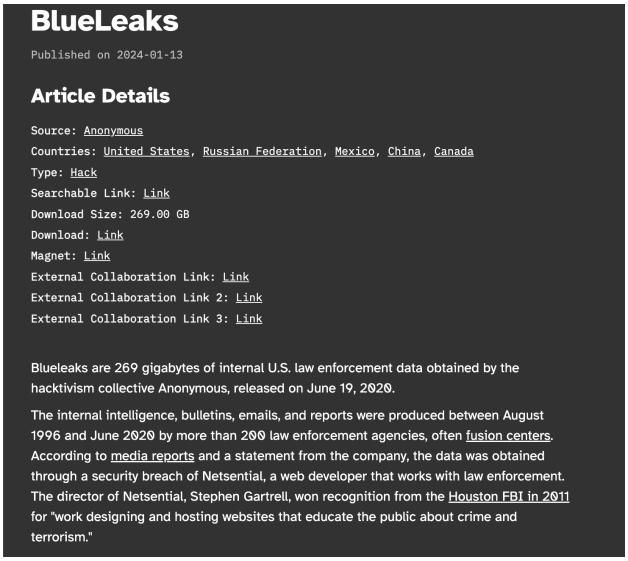
**Gamma Group / FinFisher Leak (2014):**

The same hacktivist, *Phineas Fisher*, also targeted Gamma International, FinFisher / FinSpy developer. The breach resulted in public dumps of FinFisher's surveillance code and customer documentation. The files revealed that Gamma sold its spyware to governments in Bahrain, Egypt, and Ethiopia. *finfisher-bahrain*

**BlueLeaks (2020):**

The hacktivist collective **Distributed Denial of Secrets (DDoSecrets)** published the **BlueLeaks** database — 269 GB of U.S. law enforcement and fusion center documents obtained through a compromised police contractor. While not "spyware" per se, the leak included files on surveillance

technologies, **mobile spyware contracts, facial recognition**, and **Cellebrite usage reports.** *blueleaks*




*BlueLeaks Published on DDoSecrets*

*These incidents show that spyware isn't just used by governments, it's also turned against them. Hacktivists used similar techniques (privilege escalation, exfiltration, and data publishing) to expose spyware vendors' internal workings, creating a new category of* ***counter-surveillance activism****.*

---

## Activist Groups Publishing Information on Spyware Vendors

### Citizen Lab (University of Toronto):

The academic watchdog **Citizen Lab** has been instrumental in exposing spyware operations globally. Their research teams use forensic analysis to track infections and identify responsible vendors. Major investigations include:

- Pegasus Project (with Amnesty International, 2021)
- CatalanGate (NSO & Candiru, 2022)
- Reign (QuaDream, 2023)

Citizen Lab's work provides public technical proof of infection vectors and geopolitical mapping of spyware use. *citizenlab*

**Amnesty International Security Lab:**

Amnesty's *Security Lab* provides forensic methodologies to detect Pegasus, Predator, Hermit, and FinSpy infections. Its 2021 report formed the foundation of the *Pegasus Project* and has been cited in lawsuits and government inquiries. *amnesty-research*

**Atlantic Council (Digital Forensic Research Lab – DFRLab):**

The **Atlantic Council's DFRLab** has played a major role in **analyzing and publicly documenting spyware-linked disinformation and surveillance campaigns**. Its investigations often focus on how **state and private actors weaponize digital tools for political influence and espionage**. The lab's reports have examined the operational footprints of spyware vendors, their state clients, and their impact on global cyber policy debates.

Notably, DFRLab's research on **Pegasus spyware operations** and **commercial surveillance networks** has been cited in EU and U.S. cybersecurity hearings, reinforcing the public accountability of these vendors.

| Actor | Operation | Description | Outcome / Impact | Evidence / Reference |
|---|---|---|---|---|
| APT28 (Fancy Bear) | Credential implants | Used surveillance malware on political and media targets; leaked data for disinfo. | Election interference, public exposure | *APT28 Operations* |
| APT38 (Lazarus) | Trojanized apps | Used crypto apps to monitor users and steal data. | Treasury sanctions, darknet leaks | *Treasury Sanctions* |
| FinFisher | Gamma FinFisher Leak | Dumped surveillance code and client lists from Gamma. | Exposed vendor operations | *finfisher-bahrain* |

| | | | | |
|---|---|---|---|---|
| DDoSecrets (BlueLeaks) | Law enforcement data | Published 269 GB of fusion center documents referencing Cellebrite and spyware. | Major data transparency leak | *blueleaks* |
| Citizen Lab | Pegasus / Reign / Candiru investigations | Academic forensic disclosure; global watchdog on spyware. | Legal cases, international scrutiny | *citizenlab* |
| Amnesty Security Lab | Forensic frameworks | Published Pegasus forensic methodology. | Court and NGO adoption | *amnesty-research* |
| Atlantic Council / DFRLab | Mythical Beasts & Markets Matter | Market-wide mapping of spyware vendors. | Policy recognition, EU testimony | *dfr lab* |

---

## *2.7 Legal Implications of Spyware*

The discovery of commercial spyware has pushed international law, privacy frameworks, and cybersecurity regulation into uncharted territory. As investigative journalists, digital-rights NGOs, and even private corporations expose new campaigns, governments have scrambled to close the legal loopholes that allowed surveillance tech to flourish unchecked. The legal implications now extend across **data protection**, **export control**, **human rights**, and **criminal law**, turning spyware from a technical issue into a geopolitical one.

### Has the discovery of spyware led to the enforcing of new security laws or regulations?

Yes. Major spyware revelations, particularly the Pegasus Project has triggered sweeping reforms in multiple regions:

## EU's PEGA Committee Recommendations & Telecom Regulation Push

The European Parliament's *Committee of Inquiry to Investigate the Use of Pegasus, Malware and Other Equivalent Surveillance Tools* (PEGA) has made concrete recommendations aimed at regulating how spyware or equivalent surveillance is sold and used in the EU. One media alert from PEGA outlines **eight recommendations** on telecom networks, including:

- Revoke licenses of mobile providers (2G-5G) if they facilitate unlawful access;
- Require telecom providers to deploy capabilities to detect unauthorized intrusions;
- Ensure resilience of telecom providers;
- Prevent non-EU state actors from controlling key telecom / signaling infrastructure;
- Enforce greater transparency around misuse and build legal mechanisms for reporting.

*PEGA collection*

The impact of Pegasus on fundamental rights and democratic processes

This study analyses the impact of the use of Pegasus and similar spyware on Article 2 TEU values, on privacy and data protection, and on democratic processes in Member States. It discusses the application of human rights law and EU law to spyware deployment for alleged national security purposes, focusing on the impact of spyware like Pegasus on democracy and fundamental rights. It introduces various malevolent attacks on digital devices and discusses the legal frameworks applicable to covert surveillance, including human rights instruments and EU law. Key considerations include the collection of personal data, identity theft, ransom demands, and disabling devices.

Read/download the full publication online or request hard copies by emailing us.

The use of Pegasus and equivalent surveillance spyware - The existing legal framework in EU Member States for the acquisition and use of Pegasus and equivalent surveillance spyware

This study provides a description of the legal framework (including oversight and redress mechanisms) governing the use of Pegasus and equivalent spyware in a selection of Member States. It examines the risks posed by hacking techniques to internet security and fundamental rights, focusing on tools developed by law enforcement authorities.

The study highlights the use of spyware like Pegasus by governments, raising concerns about accountability and oversight mechanisms. It identifies weaknesses in oversight in certain Member States and emphasizes the need for effective redress mechanisms for abuses of spyware. Recommendations include clearer regulation of the market for spyware, support for whistleblowers, and the adoption of clear and effective legal frameworks by Member States to ensure respect for human rights.

Read/download the full publication online or request hard copies by emailing us.

Pegasus and the EU's external relations

This study analyses the proliferation of new and emerging technologies used for repression and social control. While these technologies still have the potential to positively enhance democratic values and human rights, repressive regimes actively deploy these tools for their own strategic advantage. In particular, the proliferation of commercial spyware, such as Pegasus software, is a big concern. The EU should place a much higher priority in countering governmentuse of these tools.

Read/download the full publication online or request hard copies by emailing us.

Pegasus and surveillance spyware

This in-depth analysis looks into the confirmed or suspected use of the Pegasus spyware and other similar cybersurveillance instruments in the EU and its Member States or targeting EU citizens or residents, EU reactions and previous activities on issues related to surveillance.

Read/download the full publication online or request hard copies by emailing us.

PEGA Committee Mission to Poland

This briefing contains background materials for PEGA Committee mission to Poland. Materials collected in the briefing indicate at a large scale legislative overhaul, deep politicisation of executive branch and undermining of judicial independence that led to a paralysis in resolving flagrant violations of law due to illegal acquisition and use of Pegasus spyware in Poland. The briefing has been prepared by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the PEGA Committee.

Read/download the full publication online or request hard copies by emailing us.

*PEGA Committee publications outlining EU investigations into the use and regulation of Pegasus spyware.*

## U.S. Executive Order 14093

This EO formally prohibits U.S. federal departments and agencies from operationally using commercial spyware if it poses significant counterintelligence risk, or if the spyware vendor has been implicated in misuse or human rights abuses. Key elements:

- Agencies must **certify** that the spyware does not pose such risks before using it.
- Requires review of existing contracts to discontinue operational use of problematic spyware where possible.
- Part of a broader frame of the U.S.'s policy to align tech and democracy values, especially after the Pegasus revelations.

*commercial spyware prohibition*

## Export Controls and Entity Listing of Spyware Vendors

Already, some spyware suppliers/vendors have been put on **export control lists** or "Entity Lists," which restrict their ability to buy, sell, or receive certain technology.

- In November 2021, the U.S. Department of Commerce added **NSO Group** and **Candiru** to the Entity List under the Bureau of Industry and Security (BIS). This means any goods, technology, or software subject to U.S. export rules cannot freely go to them without a license, and license exceptions are largely denied.
- The official justification: these entities were determined to be developing or supplying spyware used by foreign governments to target journalists, activists, embassy workers, etc.

*NSO and Candiru into Entity List*

Bureau of Industry and Security
U.S. Department of Commerce

Search... Email notifications

Regulations Licensing Learn & Support News & Updates Enforcement About BIS

**FOR IMMEDIATE RELEASE** | November 4, 2021 | Media Contact: OCPA@bis.doc.gov

**Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities**

The Commerce Department's Bureau of Industry and Security (BIS) has released a final rule adding four foreign companies to the Entity List for engaging in activities that are contrary to the national security or foreign policy interests of the United States. The four entities are located in Israel, Russia, and Singapore.

NSO Group and Candiru (Israel) were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also 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. Such practices threaten the rules-based international order.

### New Policies on Visa Restrictions

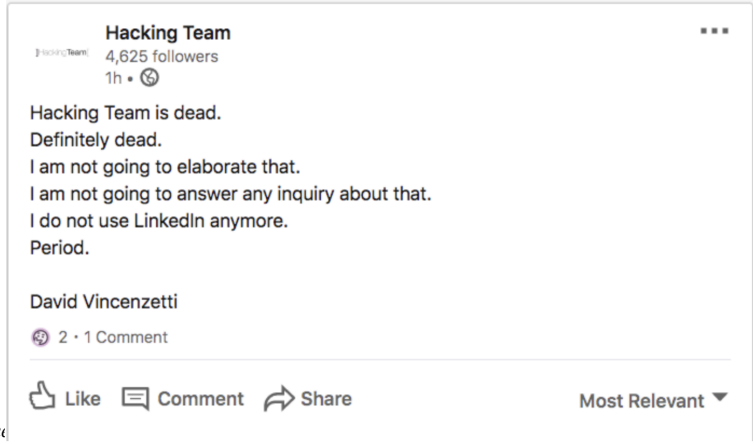
The U.S. has also adopted policies to **restrict visas** for individuals who misuse commercial spyware to target journalists, activists, dissidents, etc. This is another kind of legal tool that leverages immigration/travel law rather than export or criminal law.


---

### Has any company ceased to operate after the discovery of its spyware operations?

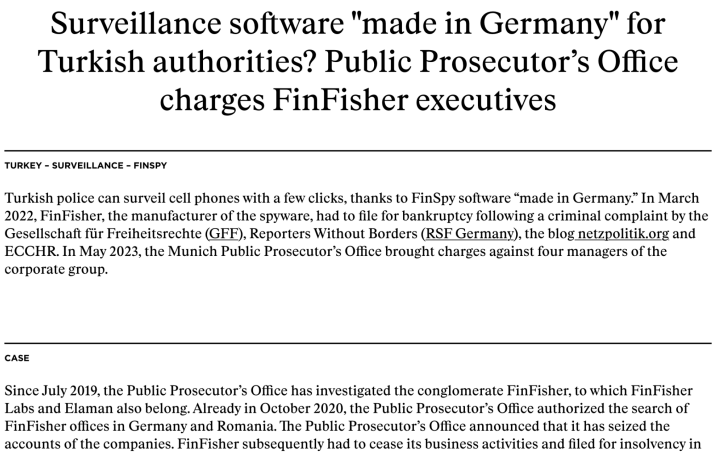
Yes, several vendors have shut down or been dismantled due to legal pressure and reputational fallout:

- **Hacking Team (Italy)**: Once a prolific surveillance software vendor, Hacking Team collapsed after a 2015 breach leaked 400 GB of internal emails and source code. The data revealed extensive global sales to repressive governments, triggering investigations and its eventual dissolution. *Hacking team is dead*




A SCREENSHOT OF THE LINKEDIN POST.

- **FinFisher (Germany/UK):** Following multiple lawsuits and raids by German authorities in 2020–2022, FinFisher declared insolvency after being accused of **illegal exports of surveillance technology** to countries like Turkey without proper licenses. *finspy insolvency*



Surveillance software "made in Germany" for Turkish authorities? Public Prosecutor's Office charges FinFisher executives

TURKEY – SURVEILLANCE – FINSPY

Turkish police can surveil cell phones with a few clicks, thanks to FinSpy software "made in Germany." In March 2022, FinFisher, the manufacturer of the spyware, had to file for bankruptcy following a criminal complaint by the Gesellschaft für Freiheitsrechte (GFF), Reporters Without Borders (RSF Germany), the blog netzpolitik.org and ECCHR. In May 2023, the Munich Public Prosecutor's Office brought charges against four managers of the corporate group.

CASE

Since July 2019, the Public Prosecutor's Office has investigated the conglomerate FinFisher, to which FinFisher Labs and Elaman also belong. Already in October 2020, the Public Prosecutor's Office authorized the search of FinFisher offices in Germany and Romania. The Public Prosecutor's Office announced that it has seized the accounts of the companies. FinFisher subsequently had to cease its business activities and filed for insolvency in

*ECCHR Article on Gamma Finfisher case leading to Insolvency*

---

### Has any company ceased to operate after the discovery of its spyware operations?

Spyware companies use legal opacity as a defense mechanism. Most structure their sales through subsidiaries, shell companies, and "lawful intercept" front entities, branding themselves as providers of digital forensic tools rather than surveillance weapons.

- Vendors typically claim compliance with national export laws, arguing that their software is sold "only to government agencies."
- Sales contracts often contain non-disclosure agreements (NDAs) and clause-based indemnity, ensuring clients remain confidential.
- They exploit gray zones in dual-use export regimes—arguing that spyware is an investigative aid, not an offensive cyber tool. *global-surveillance report*

---

### How do spyware vendors protect customer data?

In theory, vendors claim to protect client data through **on-premises deployments, encryption, and strict access controls**. In reality, many breaches and leaks prove otherwise:

- **Hacking Team and FinFisher leaks** revealed massive troves of customer data, target lists, and source code, exposing end-clients to international scrutiny.
- Some companies (e.g., NSO Group) have since claimed to adopt **"Governance, Risk, and Compliance (GRC)" frameworks**, but transparency remains limited.
- Vendors increasingly emphasize **"data sovereignty"** marketing that all captured data remains under client control, though independent audits are rare.

---

## Research notable lawsuits involving spyware suppliers and vendors

Several major lawsuits have shaped the legal landscape for spyware accountability:

**Meta (WhatsApp) vs. NSO Group (2019–2025)**

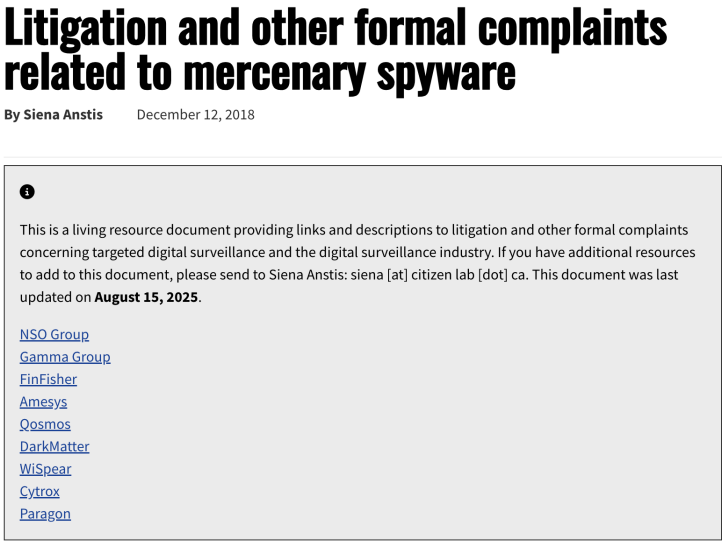
Meta sued NSO for exploiting a WhatsApp vulnerability to deploy Pegasus. The U.S. Ninth Circuit ruled that NSO is not immune from lawsuits, setting a major precedent on **foreign sovereign immunity** and private spyware firms.

**Apple vs. NSO Group (2021–Ongoing)**

Apple filed suit alleging violations of the Computer Fraud and Abuse Act (CFAA) and sought a permanent injunction. The case underscored vendor liability for "government clients' misuse."

**Citizen Lab-assisted Litigation (2023):**

Citizen Lab's research supported multiple human-rights lawsuits filed by journalists and activists targeted with Pegasus, including **WhatsApp users in India and Mexico**, expanding global jurisdiction for surveillance abuse. *litigation and formal complaints*



# Litigation and other formal complaints related to mercenary spyware

**By Siena Anstis** December 12, 2018

This is a living resource document providing links and descriptions to litigation and other formal complaints concerning targeted digital surveillance and the digital surveillance industry. If you have additional resources to add to this document, please send to Siena Anstis: siena [at] citizen lab [dot] ca. This document was last updated on **August 15, 2025**.

NSO Group
Gamma Group
FinFisher
Amesys
Qosmos
DarkMatter
WiSpear
Cytrox
Paragon

---

| Legal Action / Policy | Jurisdiction | Year | Effect / Consequence | Evidence / Reference |
|---|---|---|---|---|
| EU PEGA Recommendations | EU | 2022–24 | Proposed reforms on telecom oversight, spyware reporting, export control. | *PEGA collection* |
| US Executive Order 14093 | USA | 2023 | Banned use of risky commercial spyware by federal agencies. | *commercial spyware prohibition* |
| Entity List Sanctions (NSO, Candiru) | USA | 2021 | Restricted export of tech and components. | *NSO and Candiru into Entity List* |

| | | | | |
|---|---|---|---|---|
| Visa Restrictions Policy | USA | 2024 | Denied visas to spyware abusers. | U.S. State Department Release |
| Hacking Team Shutdown | Italy | 2015–16 | Company collapse post-leak. | *Hacking team is dead* |
| FinFisher Insolvency | Germany | 2022 | Declared bankrupt after illegal export charges. | *finspy insolvency* |
| Citizen Lab Litigation Support | Global | 2023 | NGO-backed legal precedent for spyware victims. | *litigation and formal complaints* |
| Privacy International Report | Global | 2017 | Highlighted regulatory loopholes in dual-use tech exports. | *global-surveillance report* |

---

## *2.8 The Work of Spyware Trackers*

Spyware trackers are specialized researchers, journalists, and organizations that monitor, analyze, and expose the operations of spyware vendors. Their work is crucial because commercial spyware often operates in opaque markets, targeting governments, corporations, and individuals without public oversight.

## Key Spyware Trackers & Organizations:

| Tracker / Organization | Focus Area | Notable Contributions | Methodology |
|---|---|---|---|
| Citizen Lab (University of Toronto) | Academic & NGO research | Pegasus Project (NSO), CatalanGate (NSO & Candiru), Reign (QuaDream) | Digital forensics, network traffic analysis, mobile device inspection, cross-referencing target metadata |
| Amnesty International Security Lab | Human rights & digital security | Predator Files (Intellexa), Pegasus Project | Device analysis, malware reverse engineering, forensic reporting |
| DFRLab (Atlantic Council) | Digital threat & geopolitical impact | Surveillance at the Fair, Pegasus & spyware vendor footprint analysis | OSINT, vendor mapping, expos & trade-fair tracking, public reporting |
| Google Threat Analysis Group (TAG) | Tech/telecom threats | RCS Labs Hermit exposure, Reign spyware monitoring | Vulnerability tracking, threat hunting, mobile telemetry |
| Reuters Investigative Team | Investigative journalism | DarkMatter / Project Raven exposure | Leaks, whistleblower testimony, document verification |
| The Citizen Lab & Meta / WhatsApp Collaborations | Legal advocacy & technical documentation | NSO Group lawsuits | Combining forensic analysis with legal filings and cross-jurisdictional evidence |

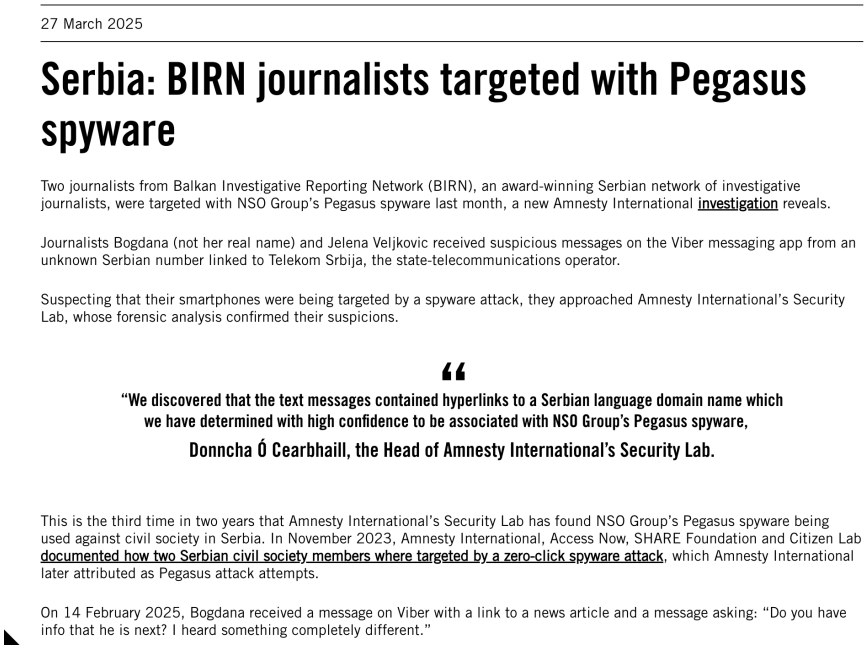
---

## Journalists Targeted by Spyware Vendors:

Investigative journalists have increasingly become targets of spyware campaigns, often linked to the very entities they investigate. These incidents underscore the escalating risks faced by the press in the digital age.

**BIRN Journalists Targeted with Pegasus, Serbia (2025)**

Two journalists from the Balkan Investigative Reporting Network (BIRN) were targeted using NSO Group's Pegasus spyware. Amnesty International's Security Lab confirmed the intrusion, highlighting the use of suspicious Viber messages containing links to Serbian domains associated with Pegasus *birn-journalists*



27 March 2025

## Serbia: BIRN journalists targeted with Pegasus spyware

Two journalists from Balkan Investigative Reporting Network (BIRN), an award-winning Serbian network of investigative journalists, were targeted with NSO Group's Pegasus spyware last month, a new Amnesty International investigation reveals.

Journalists Bogdana (not her real name) and Jelena Veljkovic received suspicious messages on the Viber messaging app from an unknown Serbian number linked to Telekom Srbija, the state-telecommunications operator.

Suspecting that their smartphones were being targeted by a spyware attack, they approached Amnesty International's Security Lab, whose forensic analysis confirmed their suspicions.

"We discovered that the text messages contained hyperlinks to a Serbian language domain name which we have determined with high confidence to be associated with NSO Group's Pegasus spyware,

**Donncha Ó Cearbhaill, the Head of Amnesty International's Security Lab.**

This is the third time in two years that Amnesty International's Security Lab has found NSO Group's Pegasus spyware being used against civil society in Serbia. In November 2023, Amnesty International, Access Now, SHARE Foundation and Citizen Lab documented how two Serbian civil society members where targeted by a zero-click spyware attack, which Amnesty International later attributed as Pegasus attack attempts.

On 14 February 2025, Bogdana received a message on Viber with a link to a news article and a message asking: "Do you have info that he is next? I heard something completely different."

*Amnesty article on Pegasus assisted investigation on BIRN Journalists*

### Italy Journalists Targeted by Paragon Solutions Spyware (2025)

Citizen Lab reported that two Italian journalists were targeted with spyware developed by Paragon Solutions, an Israeli company. The spyware, identified as "Graphite," was delivered via zero-click attacks, compromising WhatsApp communications *euro journalists*

This article is more than **4 months old**

## European journalists targeted with Paragon Solutions spyware, say researchers

**Citizen Lab says it found 'digital fingerprints' of military-grade spyware that Italy has admitted using against activists**

*Citizen Lab's article on targeted Euro Journalists with Predator Spyware*

**Dominican Republic's Investigative Journalist Targeted by NSO Spyware (2023)**
Nuria Piera, a prominent investigative journalist in the Dominican Republic, was targeted three times with NSO Group's Pegasus spyware. Amnesty International's forensic analysis confirmed the intrusions, marking a significant case of spyware use against journalists in the region *Nuria targeted*


*Nuria Piera targeted with NSO Spyware*

**Greece Journalist Targeted with Predator Spyware (2022)**
Greek journalist Thanasis Koukakis was targeted with Predator spyware, developed by the company Cytrox. An audit by Citizen Lab confirmed the infection, leading to political fallout and the resignation of key officials
*thanasis koukakis*

## Consequences for Spyware Vendors:

The discovery of spyware targeting journalists has led to significant legal and reputational consequences for the vendors involved.

**Citizen Lab-Assisted Litigation (2023)**

Citizen Lab's research supported multiple human rights lawsuits filed by journalists and activists targeted with Pegasus spyware. These lawsuits expanded global jurisdiction for surveillance abuse

**Apple vs. NSO Group (2021–Ongoing)**

Apple filed a lawsuit against NSO Group, alleging violations of the Computer Fraud and Abuse Act (CFAA) and seeking a permanent injunction. The case underscores vendor liability for the misuse of spyware by government clients

---

## *2.9 Future Trends of Spyware*

### Outlook on the Spyware Market

The commercial spyware market is expected to grow in both sophistication and geographic reach. Vendors are increasingly developing modular, multi-platform surveillance solutions that target mobile devices, cloud services, and IoT devices simultaneously. The market is likely to see further convergence with advanced cyber-intelligence tools, blurring the line between government-grade surveillance and commercial cyber-espionage products. While regulatory pressures in regions such as the EU and U.S. may slow unregulated sales, demand from governments, particularly in countries seeking authoritarian control or intelligence advantage will likely continue to drive market expansion.

### Factors Influencing Propagation

1. **Technological Advancements**
   The development of zero-click exploits, AI-assisted surveillance, and cross-platform spyware will increase operational effectiveness. Spyware capable of evading detection while automatically adapting to new security patches will accelerate market adoption.

2. **Geopolitical Dynamics**
   International conflicts, surveillance-driven state policies, and regional security threats encourage governments to procure commercial spyware. Competition between state actors for intelligence advantage will directly influence the market's propagation.

3. **Regulatory Gaps and Loopholes**
   In many regions, export controls, legal definitions of spyware, and oversight mechanisms remain inconsistent. Vendors exploit these gaps to sell spyware under the guise

of "lawful interception" tools, maintaining market access despite international scrutiny.

4. **Corporate and Critical Infrastructure Surveillance**
   Private-sector espionage and the targeting of strategic industrial or energy assets could expand the demand for spyware beyond traditional government clients. Emerging industries in AI, semiconductors, and biotechnology may increasingly become high-value targets.

## Factors Contributing to Diffusion

1. **Proliferation of Middlemen and Resellers**
   Spyware vendors are increasingly using intermediaries, front companies, and regional resellers to obscure the direct link between developer and buyer. This model reduces legal exposure while expanding distribution networks.

2. **Open-Source Intelligence (OSINT) Exposure and Leaks**
   Ironically, as spyware is repeatedly exposed through leaks and investigative reporting, its operational mechanics become publicly known. This knowledge can inadvertently aid other actors—including private criminals and competitor states—in developing or acquiring similar tools, contributing to diffusion.

3. **Cross-Platform Demand**
   With the rise of smartphones, cloud services, and IoT, spyware is adapting to a wider range of devices. Vendors increasingly market solutions capable of targeting multiple operating systems and devices from a single control panel, increasing accessibility to smaller governments or private actors.

4. **Financial Incentives**
   High-profit margins, coupled with minimal public accountability in opaque markets, make spyware development and distribution an attractive venture for new entrants, including boutique cyber-mercenary firms.

Overall, the spyware market is likely to remain highly secretive yet increasingly sophisticated, with diffusion driven by a combination of technology, geopolitical demand, regulatory gaps, and financial incentives. While legal frameworks and international scrutiny may slow growth in some regions, global demand for digital surveillance solutions will

continue to sustain market expansion.

---

## 3.1 Conclusion

This investigation shows the duality of the spyware ecosystem. On one hand, law enforcement and intelligence agencies use it for legitimate security purposes. On the other, it's often abused for political spying, corporate surveillance, and silencing dissent. Because the industry operates in secrecy and profit drives many vendors, misuse is common and accountability is rare.

From this research, several key insights stand out:

- **Spyware misuse is widespread.** Many companies that claim to sell "lawful interception" tools have been caught enabling surveillance of journalists, activists, and political opponents.

- **Corporations are not immune.** Businesses are now both targets and whistleblowers—some suffer spyware attacks, while others, like Apple and Meta, fight back through lawsuits.

- **Public exposure is powerful.** Leaks, NGO reports, and media investigations have forced transparency, leading to sanctions, lawsuits, and new laws that limit spyware abuse.

- **Regulation is improving, but uneven.** While governments are beginning to impose export controls and oversight, legal loopholes and weak enforcement still allow spyware to circulate globally.

- **The spyware market is evolving.** It's becoming more advanced, using AI, zero-click exploits, and cross-platform capabilities. At the same time, leaked tools and front companies are spreading this technology to more actors worldwide.

In conclusion, effective governance of the spyware ecosystem requires a multi-stakeholder approach, combining technological countermeasures, legal frameworks, corporate vigilance,

and public transparency to mitigate risks while preserving legitimate surveillance capabilities.

---

## ***4.1 References***

### 2.1 history

*Appearance* https://dfarq.homeip.net/spyware-invented-october-16-1995/
*Bonzi buddy* https://youtu.be/nCGD92DDsvc?si=oW1NA83WVkvfoX-7
*Back orifice* https://www.wired.com/1998/10/orifice-98/
*Coolwebsearch*
https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?Name=Spyware%3AWin32%2FCoolwebsearch.H
*Spyware goes pro*
https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

### 2.2 suppliers

*Stingray muckrock*
https://www.muckrock.com/foi/united-states-of-america-10/fbi-agreements-with-harris-corpboeing-and-meeting-minutes-re-stingrays-16083/
*Surveillance vans* https://info.publicintelligence.net/Gamma-FinFisher.pdf
*Surveillance tech at fair*
https://www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf
*Cellebrite attack*
http://www.amnestyusa.org/press-releases/serbia-authorities-using-spyware-and-cellebrite-forensic-extraction-tools-to-hack-journalists-and-activists/
*NSA ant catalog*
https://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html
*FORCEDENTRY*
https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
*Pegasus implants* https://citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022/

*Predator scandal*
*https://www.amnesty.org/en/latest/news/2023/10/global-predator-files-spyware-scandal-reveals-brazen-targeting-of-civil-society-politicians-and-officials/*
*Pegasus Hide n seek*
*https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/*
*Mythical beasts https://mythicalbeasts.dfrlab.org/*
*MB report*
*https://www.atlanticcouncil.org/in-depth-research-reports/report/mythical-beasts-and-where-to-find-them-mapping-the-global-spyware-market-and-its-threats-to-national-security-and-human-rights/*
*Candiru infra https://www.bankinfosecurity.com/candiru-spyware-infrastructure-uncovered-a-29142*
*Hooking candiru*
*https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/*
*Markets matter*
*https://www.atlanticcouncil.org/in-depth-research-reports/report/markets-matter-a-glance-into-the-spyware-industry/*
*Hacking team leak*
*https://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/*
*Serbia: a digital prison https://www.amnesty.org/en/documents/eur70/8813/2024/en/*
*Cellebrite events https://cellebrite.com/en/events/*

## 2.3 vendors

*Hermit spyware https://www.lookout.com/threat-intelligence/article/hermit-spyware-discovery*
*Rcs labs https://www.wired.com/story/hermit-spyware-rcs-labs/*
*Rcs events https://rcslab.it/en/news/cyber-intelligence-and-innovation-rcs-key-events-2025*
*quadream exploits https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/*
*iOS as target*
*https://www.washingtonpost.com/technology/2023/04/11/quadream-spyware-reports-citizen-lab/*
*Quadream shutdown https://thehackernews.com/2023/04/israeli-spyware-vendor-quadream-to-shut.html*

## 2.4 scandals

*Pegasus*
*https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/*
*Reign attack*
*https://www.spiceworks.com/it-security/endpoint-security/news/reign-spyware-iphone-ios-snooping/*
*Hacking team*
*https://www.wired.com/2015/07/hacking-team-leak-shows-secretive-zero-day-exploit-sales-work/*
*Gamma finspy https://info.publicintelligence.net/Gamma-FinFisher.pdf*
*Project raven https://www.reuters.com/investigates/special-report/usa-spying-raven/*
*Mexico pegasus exploit https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/*
*Catalangate op*
*https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/*
*Bahrain pegasus*
*https://www.amnesty.org/en/latest/news/2022/02/bahrain-devices-of-three-activists-hacked-with-pegasus-spyware/*
*Ethiopia finspy*
*https://www.amnesty.org/en/latest/research/2020/09/german-made-finspy-spyware-found-in-egypt-and-mac-and-linux-versions-revealed/*

## 2.5 corp incidents

*Whatsapp vs NSO statement*
*https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2025/01/WhatsApp-v.-NSO-Technologies.pdf*
*WhatsApp case overview*
*https://globalfreedomofexpression.columbia.edu/cases/whatsapp-inc-v-nso-group-technologies-limited-2024/*
*Apple vs NSO*
*https://www.apple.com/newsroom/pdfs/Apple_v_NSO_Complaint_112321.pdf?utm_source=chatgpt.com*
*Apple News*
*https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/*
*Jeff Bezos Phone hack*
*https://www.documentcloud.org/documents/6668313-FTI-Report-into-Jeff-Bezos-Phone-Hack/*
*Darkhotel campaign https://securelist.com/the-darkhotel-apt/66779/*
*Op aurora https://googleblog.blogspot.com/2010/01/new-approach-to-china.html*

*Mcafee night dragon*
*https://www.mcafee.com/blogs/wp-content/uploads/2011/02/McAfee_NightDragon_wp_draft_to_customersv1-1.pdf*
*Snowden article*
*https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance*

## 2.6 public disclosures

*Apt28*
*https://www.justice.gov/archives/opa/pr/grand-jury-indicts-12-russian-intelligence-officers-hacking-offenses-related-2016-election*
*Apt38 lazarus https://home.treasury.gov/news/press-releases/sm774*
*Finisher Bahrain*
*https://www.business-humanrights.org/en/latest-news/finfisher-allegedly-connected-to-bahrains-crackdown-arab-spring-activists/*
*Blueleaks https://ddosecrets.com/article/blueleaks*
*Spyware archives citizenlab https://citizenlab.ca/tag/spyware/*
*Amnesty research https://www.amnesty.org/en/latest/research/?theme=technology-and-human-rights*
*DFR LAB https://dfrlab.org/*

## 2.7 legal implications

*PEGA collection*
*https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/761472/IPOL_BRI(2024)761472_EN.pdf*
*US executive order*
*https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/*
*NSO and Candiru into entity list*
*https://www.bis.gov/press-release/commerce-adds-nso-group-other-foreign-companies-entity-list-malicious-cyber-activities*
*Hacking team shutdown https://www.vice.com/en/article/hacking-team-is-dead/*
*Finisher insolvency https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/*
*Global surveillance https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf*

*Citizen lab assisted litigations*
*https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/*

### 2.8 spyware trackers

*Birn journalists*
*https://www.amnesty.org/en/latest/news/2025/03/serbia-birn-journalists-targeted-with-pegasus-spyware/*
*Euro journalists*
*https://www.theguardian.com/media/2025/jun/12/european-journalists-targeted-with-paragon-solutions-spyware-say-researchers*
*Nuria Peira https://www.theguardian.com/world/2023/may/02/nuria-piera-spyware-target-nso-group*
*Greece Journalist*
*https://www.reuters.com/world/europe/greek-prosecutor-drops-case-against-spy-service-over-malware-use-2024-07-30/*