

NSO Group: Here for You, Here for Good

NSO Group Overview

Terrorists, drug cartels, human traffickers, sexual predators and other criminals are increasingly exploiting off-the-shelf encryption mobile messaging and communications apps, as well as other capabilities, to elude law enforcement. To stay ahead of a terrorist or pedophile who aims to perpetrate crime with a few keyboard strokes – undetected, unintercepted and unpunished – government agencies have to muster every means available.

NSO Group was founded in 2010 with a simple mission: to develop, license and support a wide-range of life-saving cyber intelligence tools to assist governments in thwarting and investigating crime and terrorism. NSO Group tools close the technological gap between government authorities and terrorists and criminals, after they “go dark” via end-to-end encryption platforms. NSO Group and its over 800 employees have developed technologies used to:

- Thwart terror attacks
- Disrupt criminal activity, including pedophilia and criminal networks, drug and human trafficking rings, gun violence, and other severe criminal acts
- Assist humanitarian search-and-rescue missions
- Protect airspace against disruptive penetration by drones.

NSO Group’s superior tools **are sold only to vetted government customers, not to individuals or private entities, for the sole use of law enforcement and intelligence agencies.** All sales of NSO Group’s technologies are subject to approval by the Israeli government and all customers are governments in the coalition of Western democracy-led countries.

NSO Group Technologies

NSO Group technologies are divided into three main categories:

- *Intelligence:* Used by dozens of vetted governments, NSO Group’s Pegasus tool provides pinpointed, target-centric, and judicious intelligence collection from mobile devices – a crucial “window” into suspects’ real-time activities. It is solely for national security or crime-fighting purposes, against a limited number of suspects, replacing traditional mass-surveillance methods.
- *Analytics:* NSO Group has developed powerful AI-based data analytics tools that ingest information from a wide variety of sensors to rapidly produce real-time insightful and actionable intelligence. That intelligence is used to sharpen the effectiveness of law enforcement activity, cybersecurity response measures, and other lawful activity.
- *Counter Drone:* Utilizing the code underpinning its other tools, NSO Group has developed a highly effective counter drone system. NSO Group’s counter drone system has the ability to quickly assume control of a drone from its operator, allowing friendly forces to safely land it and then either dispose of it or take custody of it for forensic purposes, all without jamming or creating collateral damage.

NSO Group’s technologies have saved tens of thousands of people from death, injury or exploitation. They have made our world immeasurably safer and more stable in the age of darkness created by end-to-end encryption.

NSO Group Has Developed An Unparalleled Human Rights Governance Program

NSO Group’s products are specifically designed for responsible use by law enforcement and intelligence agencies. The company does not operate the systems that it licenses to customers nor does it have access to any information such tools might yields for such customers. Its role is limited to providing “support services” entirely at the client's discretion.

NSO Group acknowledges the risk for misuse of its powerful tools in the wrong hands and is taking extraordinary steps to prevent and mitigate the risks stemming from misuse. To address potential misuse, NSO Group has developed a **human rights governance compliance program**—the first of its kind in the cyber intelligence industry. This policy subjects all end-users to a comprehensive human rights due diligence review prior to acquisition of NSO Group tools and requires contracts underlying such acquisitions to contain provisions setting forth compliance standards and human rights assurances, as well as training and other compliance requirements. Through that policy, NSO Group analyzes whether a potential government customer might use its technology to violate human rights (as defined by the United Nations and the OECD) of individuals. In addition, NSO Group is in constant contact with leading human rights advisors and academia, to constantly examine its policies and remedies.

- If analysis reveals a material possibility that a **new customer** will use NSO Group’s tools in a way that violates human rights, NSO Group will refrain from selling its tools to that specific customer.
- If misuse involving a **current customer** is alleged or discovered, NSO Group will actively investigate whether a customer is abusing human rights. If such misuse is found, NSO Group will **unilaterally disable** its systems using a “kill-switch” to prevent future abuses, as it has done multiple times in the past.
- NSO Group also strongly enforces policies developed to support internal and external whistleblowers who raise genuine concerns regarding misuse of products leading to adverse human rights impacts.

NSO Group’s top-tier legal and compliance teams have codified its commitment to ethical business, integrating human-rights safeguards in all aspects of its work – from the design to the licensing of the tools. All of these activities are subject to strong oversight from the Governance, Risks, and Compliance Committee of NSO Group’s Board of Directors. **No other cyber intelligence company offers such strong controls over advanced tools sold to law enforcement and intelligence agencies.**

These materials are distributed by Pillsbury Winthrop Shaw Pittman LLP on behalf of its foreign principal, NSO Group. Additional information is on file with the FARA Registration Unit of the Department of Justice, Washington, District of Columbia.