# NSO Group ordered to pay Meta $168 million for WhatsApp spyware attack



# NSO Group Ordered to Pay Meta Millions Following WhatsApp Spyware Campaign

In a pivotal legal decision, the Israeli surveillance firm NSO Group has been ordered to pay WhatsApp nearly $168 million in damages. This substantial judgement concludes a protracted, five-year battle that centred on NSO's exploitation of a vulnerability within the popular messaging app. The case underscored serious concerns regarding digital privacy and security, especially given that the compromised vulnerability was leveraged to target over 1,400 users, including journalists, activists, and influential figures.

The jury awarded WhatsApp $445,000 in compensatory damages alongside the punitive sum, marking a landmark victory for Meta Platforms, WhatsApp's parent company. This ruling represents a significant shift in the legal landscape surrounding the accountability of spyware developers for unlawful surveillance practices. Meta's spokesperson articulated the gravity of the situation, remarking, "Put simply, NSO’s Pegasus works to covertly compromise people’s phones with spyware capable of hoovering up information from any app installed on the device."

The implications of this ruling reach beyond mere financial penalties for NSO. The case has established a legal precedent that could deter similar illegal surveillance tactics throughout the tech industry. Notably, this trial exposed the extensive operations of NSO, revealing that the firm allocates around $50 to $60 million annually for research and development of its hacking methods. Meta's assertions were bolstered by findings from the Citizen Lab, which documented that the Pegasus spyware can evade detection by antivirus software and operate stealthily to collect sensitive data, including emails, texts, and even turn on a device’s microphone.

Despite NSO's claims that it sells its software solely to governments for counterterrorism efforts, evidence presented during the trial indicated a troubling pattern of misuse. Reports suggested that the spyware was implicated in surveillance activities across various countries, with assertions of abuses linked to authoritarian regimes in regions such as Saudi Arabia and Mexico. The testimony shed light on the dark underbelly of the spyware industry, where technology designed to bolster security can instead undermine civil liberties.

Meta has indicated plans to utilise a portion of the awarded damages to support digital rights organisations, aiming to assist those fighting against similar forms of attack globally. Despite the victory for Meta, Judge Phyllis Hamilton stated that the complexities surrounding NSO's operations could hinder the actual disbursement of damages and laid bare the ongoing issue of secrecy that envelops the firm. Reports suggested that Israeli governmental intervention had been instrumental in obstructing the release of evidence, complicating the situation further for those advocating for digital rights.

The repercussions of this verdict are likely to be profound, not only for NSO but for the wider spyware industry. Major tech firms, including Apple and Amazon, have expressed their support for WhatsApp's case, highlighting a united front among technology companies against surveillance practices that jeopardise user privacy. As digital landscapes evolve and the risks of cyber intrusions escalate, the need for robust legal frameworks to combat illegal surveillance becomes increasingly apparent.

This legal victory emphasises the necessity of vigilance in safeguarding digital privacy rights and sets a clear message that those who undermine such rights will be held accountable. The NSO case has indeed opened a crucial dialogue about the future of digital security and the ethical implications of surveillance technology.

## Reference Map:

* Paragraph 1 – [[1]](https://www.techradar.com/pro/security/nso-group-ordered-to-pay-meta-millions-following-whatsapp-spyware-campaign), [[2]](https://www.reuters.com/sustainability/society-equity/court-clash-between-meta-nso-ends-168-million-defeat-spyware-firm-2025-05-06/)
* Paragraph 2 – [[1]](https://www.techradar.com/pro/security/nso-group-ordered-to-pay-meta-millions-following-whatsapp-spyware-campaign), [[5]](https://www.ft.com/content/be26c503-b4e0-4ba5-a5ca-e9e75c351c46)
* Paragraph 3 – [[3]](https://www.reuters.com/business/meta-awarded-168-million-damages-spyware-firm-nso-group-2025-05-06/), [[4]](https://www.axios.com/2025/05/06/nso-group-whatsapp-jury-damages)
* Paragraph 4 – [[4]](https://www.axios.com/2025/05/06/nso-group-whatsapp-jury-damages), [[6]](https://www.reuters.com/business/meta-awarded-168-million-damages-spyware-firm-nso-group-2025-05-06/)
* Paragraph 5 – [[6]](https://www.reuters.com/business/meta-awarded-168-million-damages-spyware-firm-nso-group-2025-05-06/), [[7]](https://www.theguardian.com/technology/2024/dec/20/whatsapp-pegasus-spyware-nso-group-hacking)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.techradar.com/pro/security/nso-group-ordered-to-pay-meta-millions-following-whatsapp-spyware-campaign> - Please view link - unable to able to access data
2. <https://www.reuters.com/sustainability/society-equity/court-clash-between-meta-nso-ends-168-million-defeat-spyware-firm-2025-05-06/> - In a landmark legal battle, Meta Platforms secured a $168 million verdict against Israeli spyware firm NSO, concluding a six-year dispute over the illegal use of surveillance technology. The case centered around NSO's exploitation of a WhatsApp vulnerability to install spyware on users’ devices. A jury awarded Meta $444,719 in compensatory and $167.3 million in punitive damages. Meta praised the decision as a significant win for digital privacy and security, marking the first successful legal action against a spyware developer for unlawful surveillance practices. NSO, known for claiming its technology targets terrorists and criminals, expressed intent to appeal. The firm has faced global scrutiny for alleged abuses, with surveillance activities reported in several countries, including Saudi Arabia, Mexico, and Poland. The trial also revealed insights into NSO’s operations, including a $50 million research budget and its work with clients like Uzbekistan and Saudi Arabia. Despite the victory, Judge Phyllis Hamilton noted ongoing secrecy, including NSO’s resistance to evidence disclosure and Israeli government intervention to prevent document leaks to the U.S. court. The case sets a precedent for holding spyware firms accountable amidst increasing concerns over digital privacy and surveillance abuses.
3. <https://www.reuters.com/business/meta-awarded-168-million-damages-spyware-firm-nso-group-2025-05-06/> - Meta Platforms has been awarded $168 million in damages from the Israeli spyware company NSO Group. The ruling was made after NSO Group was found liable for hacking Meta's systems. Meta, the parent company of Facebook, had accused NSO of unauthorized surveillance operations that compromised its platform. The significant financial judgment reflects the seriousness of the breach and serves as a legal precedent for holding cybersecurity violators accountable. This case highlights ongoing concerns over digital privacy and the use of spyware tools.
4. <https://www.axios.com/2025/05/06/nso-group-whatsapp-jury-damages> - A California federal jury has ordered Israeli spyware company NSO Group to pay $167.25 million in punitive damages after determining the firm was responsible for hacking approximately 1,400 WhatsApp users' devices. This verdict follows a 2019 lawsuit by WhatsApp, owned by Meta, after discovering that NSO’s Pegasus surveillance software was used in the attacks. A judge had already ruled in December that NSO was liable for the hacking and breach of contract, leaving the jury to decide the amount of damages. WhatsApp hailed the decision as a significant deterrent against illegal surveillance practices targeting American companies and user privacy. The ruling marks a substantial financial blow to one of the world’s most prominent spyware vendors and sets a legal precedent that could impact similar cases in the future. Despite this legal blow, the spyware industry's growth continues to be a concern.
5. <https://www.ft.com/content/be26c503-b4e0-4ba5-a5ca-e9e75c351c46> - A U.S. federal jury has awarded WhatsApp $168 million in damages in a landmark case against NSO Group, the Israeli creator of Pegasus spyware, for exploiting a vulnerability in WhatsApp to target journalists, activists, and dissidents. This is the first time a spyware developer has been held liable for compromising a tech platform's security. The verdict sets a critical precedent for the spyware industry, which profits from exploiting software loopholes. NSO admitted spending $50–$60 million annually developing new hacking methods, and WhatsApp claimed it was one of many targets. The case was strongly supported by major tech firms like Apple and Amazon. NSO, which plans to appeal, argued its software is used by authorized governments for counterterrorism. However, WhatsApp and Citizen Lab's investigation uncovered widespread misuse, including attacks linked to authoritarian regimes. The jury trial followed a prior court ruling that NSO had violated hacking laws and WhatsApp’s terms of service. The case has drawn global attention to the spyware industry's practices and resulted in NSO being blacklisted by the Biden administration.
6. <https://www.reuters.com/business/meta-awarded-168-million-damages-spyware-firm-nso-group-2025-05-06/> - Meta Platforms has been awarded $168 million in damages from the Israeli spyware company NSO Group. The ruling was made after NSO Group was found liable for hacking Meta's systems. Meta, the parent company of Facebook, had accused NSO of unauthorized surveillance operations that compromised its platform. The significant financial judgment reflects the seriousness of the breach and serves as a legal precedent for holding cybersecurity violators accountable. This case highlights ongoing concerns over digital privacy and the use of spyware tools.
7. <https://www.theguardian.com/technology/2024/dec/20/whatsapp-pegasus-spyware-nso-group-hacking> - WhatsApp celebrates victory as judge finds Israeli company NSO Group violated state and federal US hacking laws. This article discusses the legal battle between WhatsApp and NSO Group, highlighting the court's decision and its implications for digital privacy and security.