GlobalResearch
Center for Research on Globalization

# Pegasus Rides Again: The NSO Group, Spyware and Human Rights

By Dr. Binoy Kampmark
Global Research, July 21, 2021
Region: USA
Theme: Intelligence



***

*They keep insisting they don't do it. But companies such as the Israeli NSO Group are global vendors for regimes, whatever stripe or colour, for surveillance tools to spy on those they deem of interest. The 2013 revelations by Edward Snowden that exposed the warrantless world of mass surveillance by entities such as the US National Security Agency and Britain's GCHQ caused a global rush towards encryption. Governments, left groping in the dark, sought out private providers of surveillance devices in an unregulated market. Not only could they get effective spyware; they could do so at very affordable prices.*

The NSO Group was one such provider. It sees its mission was a noble thing, marketing itself as a creator of "technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe."

The company also emphasises their mission to target those "terrorists" and "criminals" who have gone dark. "The world's most dangerous offenders communicate using technology designed to shield their communications, while government intelligence and law-enforcement agencies struggle to collect evidence and intelligence on their activities." The group insists that its "products help government intelligence and law-enforcement agencies use technology to meet the challenges of encryption to prevent and investigate terror and crime."

Forbidden Stories, a network of journalists with a mission "to protect, pursue and publish the work of other journalists facing threats, prison, or murder", sees things differently. One of the topics that figures prominently in the ranks is the Pegasus project, a collective journalism effort of global proportion coordinated by Forbidden Stories and Amnesty International's Security Lab. Its primary purpose: to expose the depredations of the Pegasus spyware, the golden child of the NSO Group.

Pegasus is a rather vicious thing, enabling those deploying it to access a phone's contents and remotely access its microphone and camera functions, turning into a surveillance device. It was given a gloss of notoriety in 2018 when it was revealed that Saudi dissident Omar Abdulaziz had been one of its victims. Abdulaziz claimed that communications with journalist Jamal Khashoggi, butchered by a Saudi squad of assassins in Istanbul in October 2018, were intercepted by the Saudi authorities because of the spyware. His lawyers

argued that the hacking "contributed in a significant manner to the decision to murder Mr. Khashoggi."

On July 18, Phineas Rueckert of Forbidden Stories revealed that some 180 journalists had been selected as targets by some 10 NSO customers across 20 countries. He begins with the Azerbaijani investigative journalist Khadija Ismayilova, whose phone was "regularly infected with Pegasus" for almost three years. Ismayilova was baffled on realising how the security of her phone had been compromised. "I feel guilty for the messages I've sent. I feel guilty for the sources who sent me [information] thinking that some encrypted messaging ways are secure and they didn't know that my phone is infected."

Details are then supplied. Both Forbidden Stories and Amnesty International were given access to a leak of more than 50,000 records of phone numbers selected by NSO clients for surveillance reasons. The clients are a varied bunch, from those of the autocratic flavour – Bahrain, Morocco and Saudi Arabia – to the more democratic ones, such as India and Mexico. The NSO Group, in a letter to Forbidden Stories, claimed it could not "confirm or deny the identity of our government customers" for "contractual and national security considerations". Rueckert admits that identifying instances where the specific phone number was compromised would be difficult short of actually analysing the device. But, with the assistance of Amnesty International's Security Lab, "forensics analyses on the phones of more than a dozen of these journalists – and 67 phones in total – [revealed] successful infections through a security flaw in iPhones as recently as this month."

The Pegasus project is significant for revealing the sheer scale of espionage. *The Guardian*, a participating media outlet, promisesto reveal more details about targets that "include lawyers, human rights defenders, religious figures, academics, businesspeople, diplomats, senior government officials and heads of state." At this writing, a rather juicy detail has come to light: the potential targeting of French President Emmanuel Macron by Morocco using Pegasus.

The NSO response to the Forbidden Stories report was snootily dismissive. The account was "full of wrong assumptions and uncorroborated theories that raise serious doubts about the reliability and interests of the sources." The company ducks the issue by suggesting that the information gathered on the individuals in question could have been obtained via other services. "The claims that the data was leaked from our servers, is a complete lie and ridiculous since such data never existed on our servers."

As for the murder of Khashoggi, old defences are resurrected. "We can confirm that our technology was not used to listen, monitor, track, or collect information regarding him or his family members mentioned in the inquiry. We previously investigated this claim, which again, is being made without validation."

For an outfit such as the NSO Group, such rebuttals have proven to be meaningless. Twin lawsuits against NSO filed in Israel and Cyprus by a Qatari citizen and by Mexican journalists in 2018 revealed extensive evidence of the company's complicity in illegal surveillance. NSO also failed to get the lawsuit by Abdulaziz dismissed, and was ordered to pay his legal costs, with the judge Guy Hyman calling the case "broad, especially in matters of the roots of constitutional values and fundamental rights". In 2019, WhatsApp brought an action against the company, claiming that Pegasus had been used to target 1400 user accounts. For WhatsApp's chief Will Cathcart, the Pegasus project reporting revealed "what we and

others have been saying for years; NSO's dangerous spyware is used to commit horrible human rights abuses all around the world and must be stopped."

The Pegasus project has shed more light on the government revolt against encryption, one facilitated by private enterprise. Left unregulated, the NSO Group and its competitors can operate with vigilante disdain and amoral proficiency. David Kaye, former UN special rapporteur on the promotion and protection of the right to freedom of opinion and expression, has wisely called for a moratorium on the sale of such spyware, describing an industry "out of control, unaccountable and unconstrained in providing governments with relatively low-cost access to the sort of spying tools that only the most advanced state intelligence services were previously able to use". Control, accountability and constraint have never quite featured in the NSO Group operations manual.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, @crg_globalresearch. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

*Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com*



---