Nana Akwasi Owusu

Dr. Snodgrass

English 102

6 March 2025

Holding NSO Group Liable for Privacy Invasion via Pegasus Spyware

In 2021, an investigation by the United Nations revealed that over 50,000 phone numbers -which included those of journalists, activists, and even some politicians- got targeted by Pegasus spyware, which is a tool that is used to infiltrate devices without the users knowing about it. Just imagine a world where someone could just gain access to your private information such as conversations, photos, location and others with just a single click or a single tap on the keyboard. This is the reality of Pegasus, which is a spyware developed by the NSO Group and is designed to be covertly and remotely installed on mobile phones running on iOS and Android. The NSO is an Israeli based company that markets its products as a tool for combating crime and terrorism. Nevertheless, Pegasus has been used pervasively and this has led to unravel its misuse and downsides. NSO must be held liable for intruding into the privacy and confidentiality of innocent citizens. The ethical consequences of mass surveillance by Pegasus, alongside its misuse of spyware and NSO’s lack of accountability and transparency prove that this technology poses a threat to global democracy if not deployed with proper boundaries. Proponents contend that tools like Pegasus are essential for national security but these claims do not consider the potential risks associated if it’s not regulated.

Arguments exist that Pegasus spyware is essential to national security and that governments use it to combat terrorism and organized crime. Critics such as the EC-Council University asserts that the Pegasus spyware has helped prevented terrorism, broken up criminal operations, and found missing persons and even assisted in searching for rescue teams. They also argue that countries such as Mexico has also benefited from the utilization of the spyware. “Mexico, the first client of the Pegasus spyware, has used it to fight the drug cartels. Notorious Mexican drug lord, Joaquin Guzman Loera, better known as El Chapo, was arrested with the help of this hacking software.” (“Pegasus”). Another argument my critics uphold is the fact that Pegasus is only sold to approved and vetted governments and as a matter of fact it is strictly monitored to ensure that is used responsibly and lawfully. Kali Robinson, a researcher and writer at the Council on Foreign Relations (CFR), contends that the NSO has licensed Pegasus to foreign law enforcement and intelligence agencies and is only sold to government agencies. In as much as these claims may seem valid and tempting, they fail to address the issues of privacy, self-regulation and the cost of surveillance.

The usage of Pegasus spyware by the various governments infringe upon the Universal Declaration of Human Rights, a law which guarantees people from getting protection from “arbitrary or random interference with privacy”. “Government using such spyware on individuals not only implicates their right to privacy but also their rights to freedom of expression and association. These rights are enshrined in international law by the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, UN Human Rights Committee documents, and the UN Guiding Principles on Business and Human Rights.” (“How NSO Group”) NSO is using Pegasus to facilitate state-sanctioned voyeurism if government agencies are permitted to hack private devices without warrants. BBC reports that the staff of French President Emmanuel Macron was targeted with Pegasus in 2021. Also, the Guardian claims that the Saudis used Pegasus to monitor the phones of those close to Jamal Khashoggi, a journalist who was assassinated in Turkey, before and after his death. This ratifies that even high-profile figures are not excluded from the diabolical use of this spyware. Beyond this, the spyware itself has designs that enables it to be systemically abused by malicious actors.