Court orders maker of Pegasus spyware to hand over code to WhatsApp

Publication Date: 2024-02-29

Author: Stephanie Kirchgaessner

Section: Technology

Tags: WhatsApp, Software, Meta, Espionage, Israel, news

Article URL: https://www.theguardian.com/technology/2024/feb/29/pegasus-surveillance-code-whatsapp-meta-lawsuit-nso-group

NSO Group, the maker of one the world's most sophisticated cyber weapons, has been ordered by a US court to hand its code for Pegasus and other spyware products to WhatsApp as part of the company's ongoing litigation. The decision by Judge Phyllis Hamilton is a major legal victory for WhatsApp, the Meta-owned communication app which has been embroiled in a lawsuit against NSO since 2019, when it alleged that the Israeli company's spyware had been used against 1,400 WhatsApp users over a two-week period. NSO's Pegasus code, and code for other surveillance products it sells, is seen as a closely and highly sought state secret. NSO is closely regulated by the Israeli ministry of defence, which must review and approve the sale of all licences to foreign governments. In reaching her decision, Hamilton considered a plea by NSO to excuse it of all its discovery obligations in the case due to "various US and Israeli restrictions". Ultimately, however, she sided with WhatsApp in ordering the company to produce "all relevant spyware" for a period of one year before and after the two weeks in which WhatsApp users were allegedly attacked: from 29 April 2018 to 10 May 2020. NSO must also give WhatsApp information "concerning the full functionality of the relevant spyware". Hamilton did, however, decide in NSO's favor on a different matter: the company will not be forced at this time to divulge the names of its clients or information regarding its server architecture. "The recent court ruling is an important milestone in our long-running goal of protecting WhatsApp users against unlawful attacks. Spyware companies and other malicious actors need to understand they can be caught and will not be able to ignore the law," a WhatsApp spokesperson said. NSO declined to comment on the decision. The litigation is continuing. When it is successfully deployed against a target, NSO's Pegasus software can hack any mobile phone, gaining unrestricted access to phone calls, emails, photographs, location information and encrypted messages without a user's knowledge. NSO was blacklisted by the Biden administration in 2021 after it determined the Israeli spyware maker has acted "contrary to the foreign policy and national security interests of the US". NSO sells its spyware to government clients around the world and has said that the agencies who deploy it are responsible for how it is used. While NSO does not disclose the names of its clients, research and media reports over the years have identified Poland, Saudi Arabia, Rwanda, India, Hungary and the United Arab Emirates as among the countries that have previously used the technology to target dissidents, journalists, human rights activists and other members of civil society. NSO has argued that Pegasus helps law enforcement and intelligence agencies fight crime and protect national security and that its technology is intended to help catch terrorists, child abusers and hardened criminals. The Biden administration has raised alarms about the proliferation and abuse of products like Pegasus, saying they represent a potential threat to US national security and

counterintelligence efforts. A new policy unveiled in early February will impose global visa restrictions on individuals who have been involved in the misuse of commercial spyware, including countries in the EU and Israel.