The Guardian

Israeli firm linked to WhatsApp spyware attack faces lawsuit

Amnesty International fears its staff may be 'surveilled via NSO Pegasus software'

Dan Sabbagh

Sat 18 May 2019 06.00 BST

The Israeli firm linked to this week's WhatsApp hack is facing a lawsuit backed by Amnesty International, which says it fears its staff may be under surveillance from spyware installed via the messaging service.

The human rights group's concerns are detailed in a lawsuit filed in Israel by about 50 members and supporters of Amnesty International Israel and others from the human rights community. It has called on the country's ministry of defence to ban the export of NSO's Pegasus software, which can covertly take control of a mobile phone, copy its data and turn on the microphone for surveillance.

An affidavit from Amnesty is at the heart of the case, and concludes that "staff of Amnesty International have an ongoing and well-founded fear they may continue to be targeted and ultimately surveilled" after a hacking attempt last year.

NSO Group, founded in 2010, supplies industry-leading surveillance software to governments that it says is for tackling terrorism and serious crime, and has been licensed to dozens of countries including Saudi Arabia, Mexico, Bahrain and the UAE.

But there have been a string of complaints in the past few months, documented largely by the Toronto-based Citizen Lab, that the technology has been used to target human rights groups, activists and journalists by several countries - and that there has been no attempt to rein it in.

That culminated, earlier this week, in the announcement by Facebook-owned WhatsApp that it had raced to patch up a security hole in its messaging service, which it believed had been exploited by NSO Group, that would have allowed spyware to be placed on a person's mobile phone simply via a missed WhatsApp call.

That represents a technical step beyond the breaches reported by Amnesty in its lawsuit, although it is not the first time that NSO has been accused of exploiting WhatsApp to hack phones.

Last June, an Amnesty staffer received "a suspicious message over WhatsApp", according to the affidavit. The recipient was asked to cover the protest "for your brothers detained in Saudi Arabia in front of the Saudi embassy in Washington" and invited to click a link.

Technical analysis indicated the link was part of "a network of digital infrastructure comprising more than 600 suspicious domains used to lure targeted individuals to click on links that trigger infection with Pegasus spyware" onto a target's mobile phone, it said.

Such links often aim to impersonate news sites by using slightly misspelled domain names or different suffixes, for example replacing .com with .net.

The Israeli government's Defence Export Controls Agency has failed to exercise proper oversight "despite serious allegations of abuse", the affidavit claimed, adding: "Because of DECA's inaction, NSO Group can continue to sell its software to governments known to target human rights defenders."

It is the latest in a string of Israeli lawsuits faced by the company. Omar Abdulaziz, a Saudi dissident based in Montreal, last December filed a lawsuit in Israel in which he claimed that NSO software had been used to target his phone at a time when he was in regular contact with the journalist Jamal Khashoggi.

In October, Khashoggi is believed to have been killed and dismembered at the Saudi consulate in Istanbul, Turkey - although the Middle Eastern country's government still denies involvement. Saudi Arabia is understood to have licensed NSO technology in 2017, paying $55m for the technology, according to Israeli news reports.

NSO said it wants to "do whatever is necessary" to ensure its technology is used for fighting terrorism and serious crime and "not abused in a manner that undermines other equally fundamental human rights". Its response came in a 26-page reply sent earlier this week to Amnesty and Citizen Lab from the British venture capital firm that is now its parent company.

Three months ago, a majority stake in NSO was acquired by the London based firm Novalpina Capital, founded by the banker and philanthropist Stephen Peel. It appears eager to rehabilitate the controversial software company's reputation and maintain its value.

The lengthy reply to Amnesty, signed by Peel, claimed that in "almost all" the cases of complaints of human rights abuse raised, the alleged victim of hacking had not been a target or the government in question had acted with "due lawful authority".

A statement that has been challenged by Amnesty. Danna Ingleton, the deputy director of Amnesty's technology division, said: "We believe that the reality is different. We've seen them target human rights organisations and no evidence they've been able to effectively control governments when complaints have been raised."

Profile: Stephen Peel

Peel, a former Olympic rower who competed in the Seoul Olympics, is a long-term financier who set up Novalpina in 2016 after stints at the investment bank Goldman Sachs and the US private equity giant TPG.

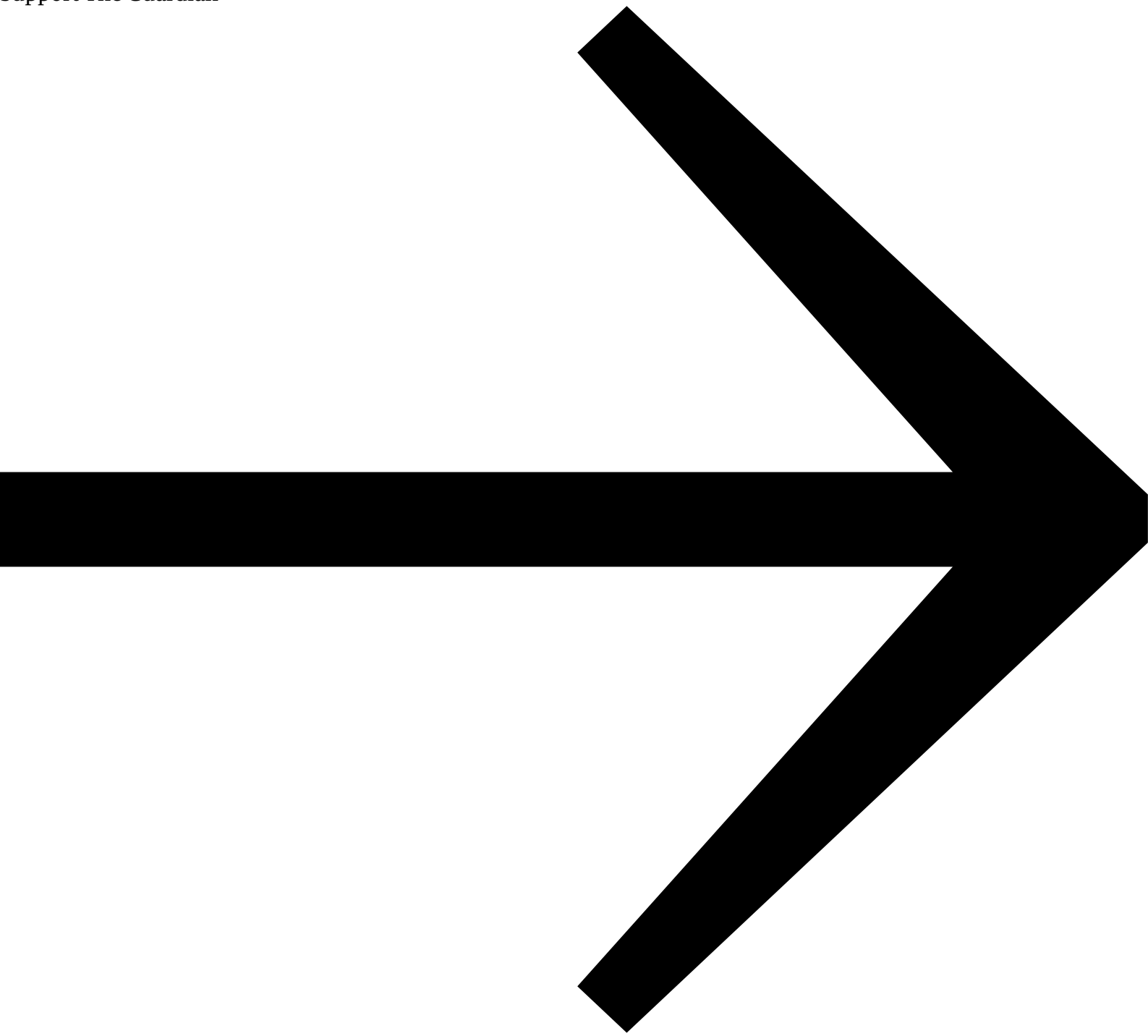
In recent years he has become a philanthropist as well, sitting on a number of boards, and said last year he had donated £100,000 to the anti-Brexit campaign group Best for Britain.

"We have heard the strident calls from those against us to try and close down debate and silence discussion over the disaster that Brexit appears to be. I for one, will not be silenced," he said in an interview with the Observer.

However, Peel stood down from the board of Global Witness, a human rights and environmental campaigning organisation in February, after the buyout of NSO.

The statement announcing Peel's departure described his decision as "typically selfless" - although there is understood to have been considerable concern in some quarters of the organisation once the acquisition was confirmed.

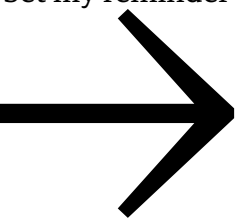
Support The Guardian



Remind me in September

Remind me in September
Email address

Set my reminder



We will use this to send you a single email in September 2020. To find out what personal data we collect and how we use it, please visit our Privacy Policy

We will be in touch to invite you to contribute. Look out for a message in your inbox in September 2020. If you have any questions about contributing, please contact us here.

Topics

- Surveillance
- WhatsApp
- Amnesty International
- Israel
- Malware
- Data and computer security
- Privacy
- news