

Human Rights and surveillance: Edward Snowden calls for spyware trade ban amid Pegasus revelations

Wednesday 21 July 2021, by [LEWIS Paul](#), [PEGG David](#) (Date first published: 19 July 2021).

NSA whistleblower warns of world in which no phone is safe from state-sponsored hackers if no action taken.

[Edward Snowden on spyware: 'This is an industry that should not exist' - video]

Governments must impose a global moratorium on the international spyware trade or face a world in which no mobile phone is safe from state-sponsored hackers, [Edward Snowden](#) has warned in the wake of revelations about the clients of NSO Group.

Snowden, who [in 2013 blew the whistle](#) on the secret mass surveillance programmes of the US National Security Agency, described for-profit malware developers as “an industry that should not exist”.

He made the comments in an interview with the Guardian after the first [revelations from the Pegasus project](#), a journalistic investigation by a consortium of international media organisations into the NSO Group and its clients.

NSO Group manufactures and sells to governments advanced spyware, branded as Pegasus, that can [secretly infect a mobile phone and harvest its information](#). Emails, texts, contact books, location data, photos and videos can all be extracted, and a phone’s microphone and camera can be activated to covertly record the user.

The consortium analysed a leaked dataset of 50,000 phone numbers that, it is believed, were identified as belonging to persons of interest to NSO’s customers. Forensic analysis of a sample of the mobile phones found dozens of cases of successful and attempted Pegasus infections.

NSO Group says it takes ethical considerations seriously, is regulated by the export control regimes of [Israel](#), Cyprus and Bulgaria and only sells to vetted government clients. But its customers have included repressive regimes, including Saudi Arabia, the United Arab Emirates and Azerbaijan.

Speaking in an interview with the Guardian, Snowden said the consortium’s findings illustrated how commercial malware had made it possible for repressive regimes to place vastly more people under the most invasive types of surveillance.

[Video: Pegasus: the spyware technology that threatens democracy]

For traditional police operations to plant bugs or wiretap a suspect’s phone, law enforcement would need to “break into somebody’s house, or go to their car, or go to their office, and we’d like to think they’ll probably get a warrant”, he said.

But commercial spyware made it cost-efficient for targeted surveillance against vastly more people. "If they can do the same thing from a distance, with little cost and no risk, they begin to do it all the time, against everyone who's even marginally of interest," he said.

"If you don't do anything to stop the sale of this technology, it's not just going to be 50,000 targets. It's going to be 50 million targets, and it's going to happen much more quickly than any of us expect."

Part of the problem arose from the fact that different people's mobile phones were functionally identical to one another, he said. "When we're talking about something like an iPhone, they're all running the same software around the world. So if they find a way to hack one iPhone, they've found a way to hack all of them."

He compared companies commercialising vulnerabilities in widely used mobile phone models to an industry of "infectioneers" deliberately trying to develop new strains of disease.

[Graph: What is Pegasus spyware and how does it hack phones?]

"It's like an industry where the only thing they did was create custom variants of Covid to dodge vaccines," he said. "Their only products are infection vectors. They're not security products. They're not providing any kind of protection, any kind of prophylactic. They don't make vaccines - the only thing they sell is the virus."

Snowden said commercial malware such as Pegasus was so powerful that ordinary people could in effect do nothing to stop it. Asked how people could protect themselves, he said: "What can people do to protect themselves from nuclear weapons?"

"There are certain industries, certain sectors, from which there is no protection, and that's why we try to limit the proliferation of these technologies. We don't allow a commercial market in nuclear weapons."

He said the only viable solution to the threat of commercial malware was an international moratorium on its sale. "What the Pegasus project reveals is the NSO Group is really representative of a new malware market, where this is a for-profit business," he said. "The only reason NSO is doing this is not to save the world, it's to make money."

He said a global ban on the trade in infection vectors would prevent commercial abuse of vulnerabilities in mobile phones, while still allowing researchers to identify and fix them.

"The solution here for ordinary people is to work collectively. This is not a problem that we want to try and solve individually, because it's you versus a billion dollar company," he said. "If you want to protect yourself you have to change the game, and the way we do that is by ending this trade."

NSO Group [said in a series of statements](#) that it rejected "false claims" about the company and its clients, and said it did not have visibility over its clients use of Pegasus spyware. It said it only sold the software to vetted government clients, and that its technology had helped to prevent terrorism and serious crime.

Following the launch of the Pegasus project, Shalev Hulio, the founder and chief executive of NSO, said he continued to dispute that the leaked data "has any relevance to NSO", but added that he was "very concerned" about the reports and promised to investigate them all. "We understand that in some circumstances our customers might misuse the system," he said.

David Pegg and Paul Lewis

P.S.

- The Guardian. Mon 19 Jul 2021 15.00 BST :
<https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations>

- Support the Guardian
Available for everyone, funded by readers

[Contribute](#)

[Subscribe](#)