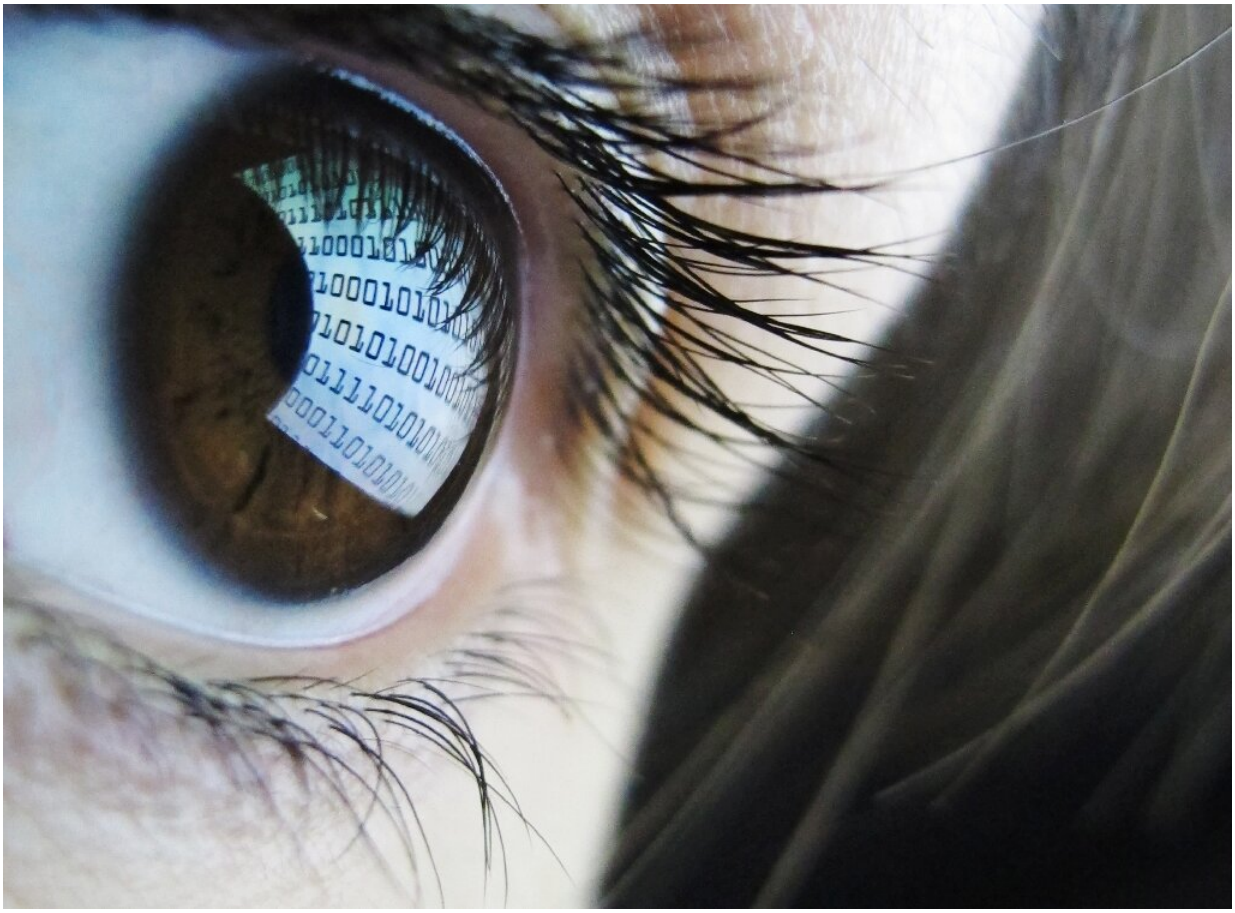
Spyware for sale: the booming trade in surveillance tech

July 22 2021, by Katy Lee



Calls are growing for greater regulation, or even a moratorium on over-intrusive surveillance technology.

Israeli's NSO Group is in the eye of a storm over its Pegasus

spyware—but it is far from the only company helping governments with their covert surveillance operations.

Explosive claims that Pegasus was used to spy on activists and even heads of state have shone a spotlight on the software, which allows highly intrusive access to a person's mobile phone.

But NSO are merely one player in an industry that has quietly boomed in recent years, arming even cash-strapped governments with powerful surveillance technology.

"These tools have gotten cheaper and cheaper," said Allie Funk, senior research analyst in technology and democracy at the US think tank Freedom House.

"So it's not just the world's foremost intelligence agencies that can purchase them—it's smaller governments, or local police agencies."

Emerging economies such as India, Mexico and Azerbaijan dominate the list of countries where large numbers of phone numbers were allegedly identified as possible targets by NSO's clients.

Ron Deibert, director of the University of Toronto's Citizen Lab research centre, said such companies allowed governments to effectively "purchase their own NSA"—a nod to the US National Security Agency, whose own extensive surveillance was exposed by Edward Snowden.

The Citizen Lab scours the internet for traces of digital espionage by governments.

Just last week it published an investigation into another secretive Israeli company that sells spyware to foreign governments, Candiru.

It appears to have been similarly used to target dissidents and journalists, from Turkey to Singapore.

And in 2017, Citizen Lab found that Ethiopia had used spyware developed by Cyberbit—yet another Israeli firm—to infect the computers of exiled dissidents.

'Entrepreneurial' ex-spies

"There are multiple factors why we see a lot of Israeli companies," Deibert said.

One is the "openly entrepreneurial" attitude of Israel's cyber-espionage agency Unit 8200, who "encourage their graduates to go out and develop start-ups after their military service", he told AFP.

He added there was "a strong suspicion" that Israel gains "strategic intelligence" from this technology being provided to other governments, siphoning off some of the information gathered.

But while Israel is now facing calls for an export ban on such technology, it is not the only country hosting companies that sell off-the-shelf spyware.

Like Pegasus, Germany's FinFisher is marketed as a tool to help intelligence and law enforcement agencies to fight crime.

But it, too, has faced accusations that it has been used for abusive surveillance, including to spy on Bahraini journalists and activists.

Italian firm Hacking Team was at the centre of its own Pegasus-style scandal in 2015 when a leak revealed it was selling spyware to dozens of governments worldwide. It has since been rebranded as Memento Labs.

Not all companies in this shadowy industry specialise in the same kind of technology.

Some sell tools that mimic cell phone towers, helping authorities to intercept phone calls; others, such as Cellebrite, have helped police forces from the US to Botswana to crack into locked mobile phones.

Grey zone

Deibert drew a distinction between companies operating in this "lawful interception" industry and "hack for hire" outfits—borderline criminal groups "that do hacking on behalf of states".

Analysts suspect, however, that spyware companies lean frequently on hackers' expertise.

Recent versions of Pegasus have used weak spots in software commonly installed on smartphones—such as WhatsApp and Apple's iMessage—in order to install the spyware on people's devices.

While it remains unclear how NSO's developers discovered these weak spots, hackers commonly sell access to these so-called "zero-day vulnerabilities" on the dark web.

"NSO has done a lot of research and development, but it also relies on the grey market for vulnerabilities," said French cybersecurity expert Loic Guezo.

He said companies like Zerodium in the US buy access to these software vulnerabilities from hackers and sell them either directly to states or to companies like NSO.

As the Pegasus scandal rumbles on, calls are growing for the industry to

face greater regulation—or even a moratorium on this kind of surveillance technology altogether.

But for Deibert, "the reality is that almost all governments have a stake in keeping this industry the way it is—secretive, unregulated—because they benefit by it".

"So it will take a lot to bring about the sort of moratorium that my colleagues are calling for," he said.