Meet Toka, the Most Dangerous Israeli Spyware Firm You've Never Heard Of

Meet Toka, the Most Dangerous Israeli Spyware Firm You've Never Heard Of

> ***The mainstream media's myopic focus on Israel's Pegasus spyware and the threats it poses means that other companies, like Toka, go uninvestigated, even when their products present an even greater potential for abuse and illegal surveillance.***

by **Whitney Webb**, *Mint Press News*
July 21, 2021

LONDON – This past Sunday, an investigation into the global abuse of spyware developed by veterans of Israeli intelligence Unit 8200 gained widespread attention, as it was revealed that the software – sold to democratic and authoritarian governments alike – had been used to illegally spy on an estimated 50,000 individuals. Among those who had their communications and devices spied on by the software, known as Pegasus, were journalists, human rights activists, business executives, academics and prominent political leaders. Among those targeted political leaders, per reports, were the current leaders of France, Pakistan, South Africa, Egypt, Morocco and Iraq.

The abuse of Pegasus software in this very way has been known for several years, though these latest revelations appear to have gained such traction in the mainstream owing to the high number of civilians who have reportedly been surveilled through its use. The continuation of the now-years-

long scandal surrounding the abuse of Pegasus has also brought considerable controversy and notoriety to the Israeli company that developed it, the NSO Group.

While the NSO Group has become infamous, other Israeli companies with even deeper ties to Israel's intelligence apparatus have been selling software that not only provides the exact same services to governments and intelligence agencies but purports to go even farther.

Originally founded by former Israeli Prime Minister and Jeffrey Epstein associate Ehud Barak, one of these companies' wares are being used by countries around the world, including in developing countries with the direct facilitation of global financial institutions like the Inter-American Development Bank (IDB) and the World Bank. In addition, the software is only made available to governments that are "trusted" by Israel's government, which "works closely" with the company.

Despite the fact that this firm has been around since 2018 and was covered in detail by this author for *MintPress News* in January 2020, no mainstream outlet – including those that have extensively covered the NSO Group – has bothered to examine the implications of this story.

> *How Government and Media Are Prepping America for a Failed 2020 Election*

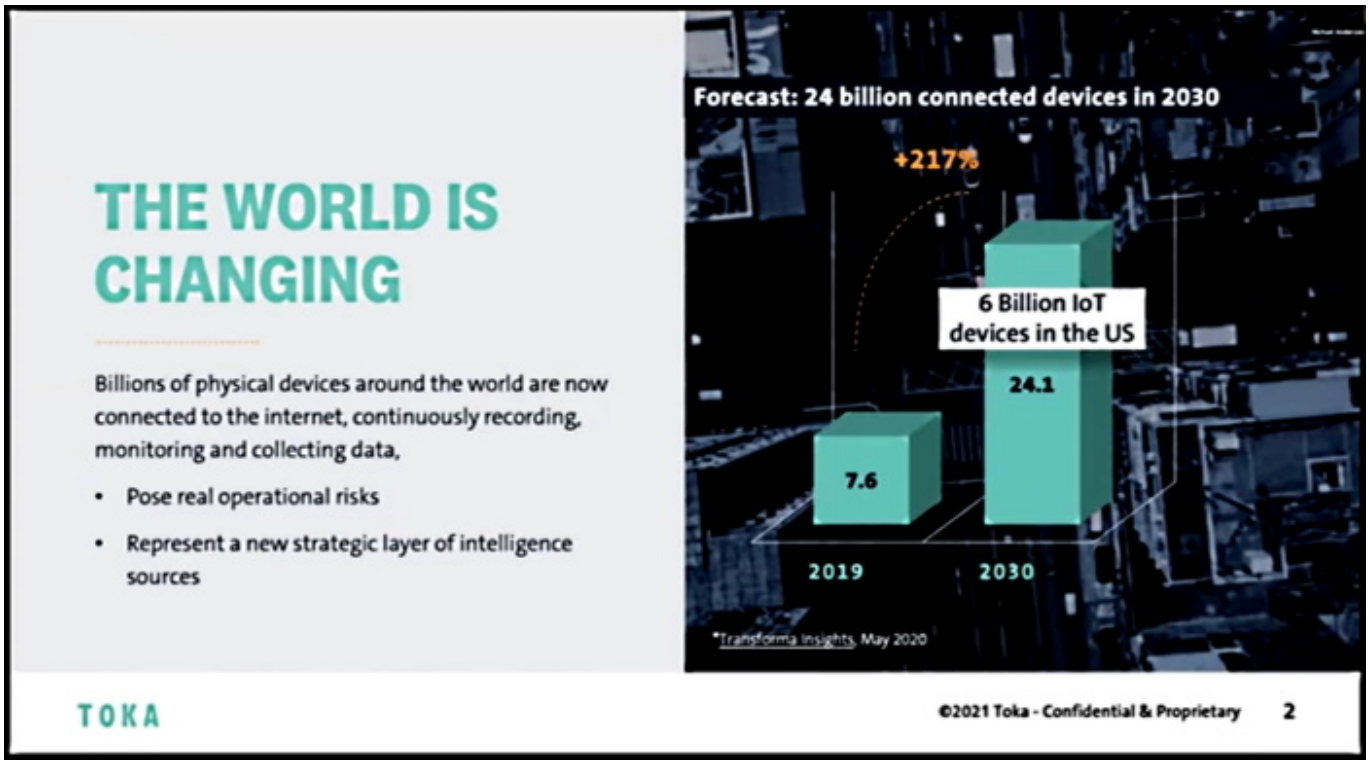
Worse than Pegasus

Toka was launched in 2018 with the explicit purpose of selling a "tailored ecosystem of cyber capabilities and software products for governmental, law enforcement, and security agencies." According to a profile of the company published in *Forbes* shortly after it launched, Toka advertised itself as "a one-stop hacking shop for governments that require extra capability to fight terrorists and other threats to national security in the digital domain."

Toka launched with plans to “provide spy tools for whatever device its clients require,” including not only smartphones but a “special focus on the so-called Internet of Things (IoT).” Per the company, this includes devices like Amazon Echo, Google Nest-connected home products, as well as connected fridges, thermostats and alarms. Exploits in these products discovered by Toka, the company said at the time, would not be disclosed to vendors, meaning those flaws would continue to remain vulnerable to any hacker, whether a client of Toka or not.

Today, Toka’s software suite claims to offer its customers in law enforcement, government and intelligence the ability to obtain “targeted intelligence” and to conduct “forensic investigations” as well as “covert operations.” In addition, Toka offers governments its “Cyber Designers” service, which provides “agencies with the full-spectrum strategies, customized projects and technologies needed to keep critical infrastructure, the digital landscape and government institutions secure and durable.”

Given that NSO’s Pegasus targets only smartphones, Toka’s hacking suite – which, like Pegasus, is also classified as a “lawful intercept” product – is capable of targeting *any* device connected to the internet, including but not limited to smartphones. In addition, its target clientele are the same as those of Pegasus, providing an easy opportunity for governments to gain access to even more surveillance capabilities than Pegasus offers, but without risking notoriety in the media, since Toka has long avoided the limelight.



In addition, while Toka professes that its products are only used by "trusted" governments and agencies to combat "terrorism" and maintain order and public safety, the sales pitch for the NSO Group's Pegasus is remarkably similar, and that sales pitch has not stopped its software from being used to target dissidents, politicians and journalists. It also allows many of the same groups who are Toka clients, like intelligence agencies, to use these tools for the purpose of obtaining blackmail. The use of blackmail by Israeli security agencies against civilian Palestinians to attempt to weaken Palestinian society and for political persecution is well-documented.

Toka has been described by market analysts as an "offensive security" company, though the company's leadership rejects this characterization. Company co-founder and current CEO Yaron Rosen asserted that, as opposed to purely offensive, the company's operations are "something in the middle," which he classifies as bridging cyber defense and offensive cyber activities – e.g., hacking.

The company's activities are concerning in light of the fact

that Toka has been directly partnered with Israel's Ministry of Defense and other Israeli intelligence and security agencies since its founding. The company "works closely" with these government agencies, according to an Israeli Ministry of Defense website. This collaboration, per Toka, is meant to "enhance" their products. Toka's direct IDF links are in contrast to the NSO Group, a company that does not maintain overt ties with the Israeli security state.

Toka's direct collaboration with Israel's government is also made clear through its claim that it sells its products and offers its services only to "trusted" governments, law enforcement agencies and intelligence agencies. Toka's Rosen has stated that Russia, China, and "other enemy countries" would never be customers of the company. In other words, only countries aligned with Israeli policy goals, particularly in occupied Palestine, are permitted to be customers and gain access to its trove of powerful hacking tools. This is consistent with Israeli government efforts to leverage Israel's hi-tech sector as a means of countering the Boycott, Divest and Sanctions (BDS) movement globally.

Further evidence that Toka is part of this Israeli government effort to seed foreign governments with technology products deeply tied to Israel's military and intelligence services is the fact that one of the main investors in Toka is Dell Technologies Capital, which is an extension of the well-known tech company Dell. Dell was founded by Michael Dell, a well-known pro-Israel partisan who has donated millions of dollars to the Friends of the IDF and is one of the top supporters of the so-called "anti-BDS" bills that prevent publicly employed individuals or public institutions in several U.S. states from supporting non-violent boycotts of Israel, even on humanitarian grounds. As *MintPress* previously noted, the fact that a major producer of consumer electronic goods is heavily investing in a company that markets the hacking of that very technology should be a red flag.

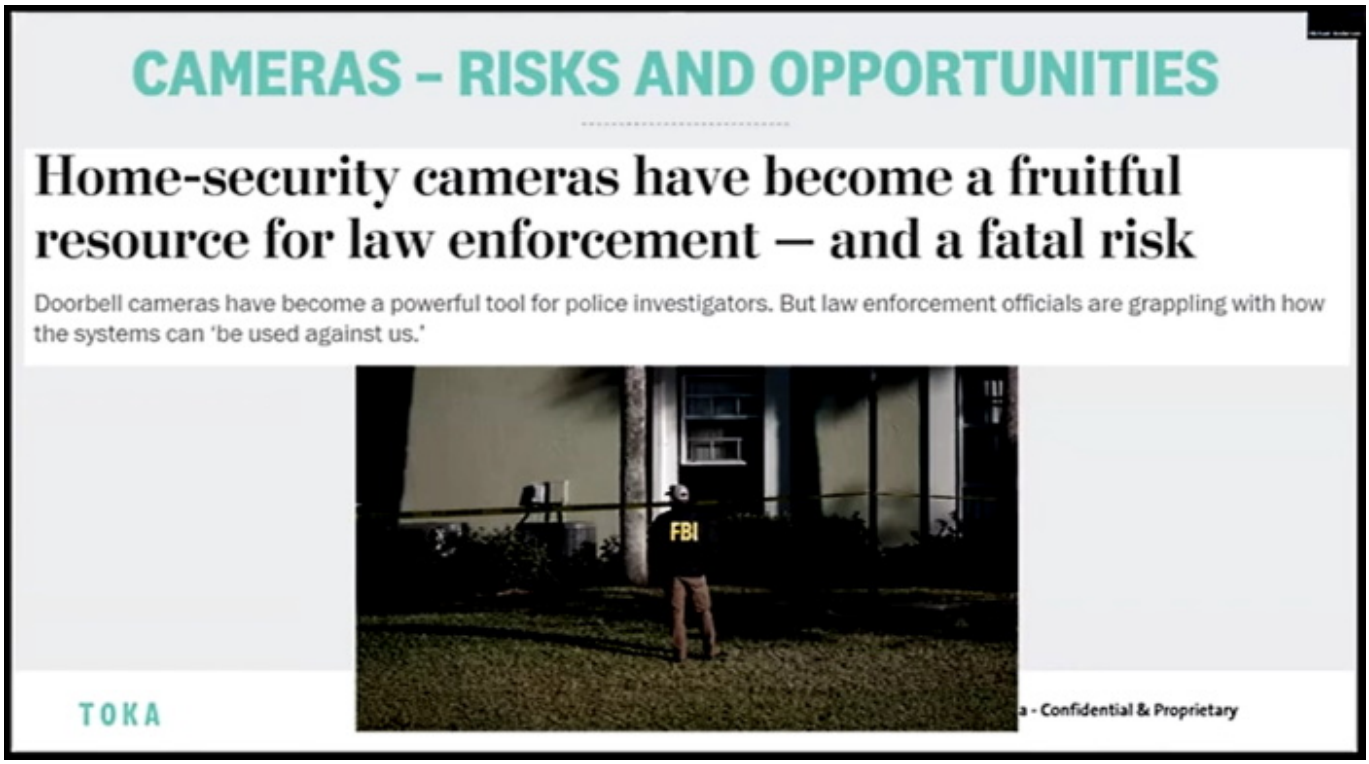
The government's initial admitted use of the hi-tech sector to counter the BDS movement coincided with the launch of a new Israeli military and intelligence agency policy in 2012,

whereby “cyber-related and intelligence projects that were previously carried out in-house in the Israeli military and Israel’s main intelligence arms are transferred to companies that, in some cases, were built for this exact purpose.”

One of the reasons this was reportedly launched was to retain members of Unit 8200 engaged in military work who were moving to jobs in the country’s high-paying tech sector. Through this new policy that has worked to essentially merge much of the private tech sector with Israel’s national security state, some Unit 8200 and other intelligence veterans continue their work for the state but benefit from a private sector salary. The end result is that an unknown – and likely very high – number of Israeli tech companies are led by veterans of the Israeli military and Israeli intelligence agencies and serve, for all intents and purposes, as front companies. A closer examination of Toka strongly suggests that it is one such front company.

Toka – born out of Israel’s national security state

The company was co-founded by Ehud Barak, Alon Kantor, Kfir Waldman and retired IDF Brigadier General Yaron Rosen. Rosen, the firm’s founding CEO and now co-CEO, is the former Chief of the IDF’s cyber staff, where he was “the lead architect of all [IDF] cyber activities,” including those executed by Israeli military intelligence Unit 8200. Alon Kantor is the former Vice President of Business Development for Check Point Software, a software and hardware company founded by Unit 8200 veterans. Kfir Waldman is the former CEO of Go Arc and a former Director of Engineering at technology giant Cisco. Cisco is a leader in the field of Internet of Things devices and IoT cybersecurity, while Go Arc focuses on applications for mobile devices. As previously mentioned, Toka hacks not only mobile devices but also has a “special focus” on hacking IoT devices.



In addition to having served as prime minister of Israel, Toka co-founder Ehud Barak previously served as head of Israeli military intelligence directorate Aman, as well as several other prominent posts in the IDF, before eventually leading the Israeli military as minister of defense. While minister of defense, he led Operation Cast Lead against the blockaded Gaza Strip in 2009, which resulted in the deaths of over 1,000 Palestinians and saw Israel illegally use chemical weapons against civilians.

Read the rest of the article at Mint Press News

Connect with Mint Press News

cover image credit: Antonio Cabrera / Mint Press News