Surveillance as a Service: The Global Impact of Israeli "Defense" Technologies on Privacy and Human Rights | Tor Project

10-12 minutes

Highlighting, exposing, and actively working against the proliferation and normalization of surveillance technology is crucial in protecting human rights worldwide. At the Tor Project, we know that it is through collective awareness and action that we can all build and contribute to privacy-preserving technologies that aim to protect people everywhere from the prevalence of surveillance and oppression. It is equally important to hold companies accountable and recognize the source and enablers of surveillance tech, especially now as we see these technologies being aggressively utilized in the ongoing genocide in Gaza.

This post delves into the impact of Israeli surveillance technologies in Palestine, illustrating how localized instances of its use can have extensive repercussions that pave the way for the widespread acceptance and global adoption of such oppressive practices.

There is a growing need for a global stance against the use of technology for oppression. Tech workers and the broader international community are urged to prioritize integrity over profit to protect privacy and prevent the deleterious impacts of pervasive surveillance on our lives. There is even more urgency to address these issues in the face of growing demand for surveillance solutions enhanced and exacerbated by AI.

Global Surveillance and Oppression

The examples below demonstrate the alarming sophistication of surveillance capitalism and its increasingly global footprint. They also explore how Israeli spyware and surveillance companies navigate global scrutiny by rebranding and establishing offices worldwide, all while a network of venture capital firms facilitate their operations and help them avoid much needed accountability.

- Elbit Systems is a leading military tech exporter in Israel, specializing in various advanced surveillance technologies, terrifyingly deployed in space, air, sea and ground operations. Its surveillance systems, drones, and other high-tech tools, which are used to enforce violent occupations and apartheid, are in high demand worldwide.

- This pervasive surveillance technology doesn't end in Palestine, but it often starts with it.

- Since at least 2014, Elbit Systems has been deploying these tools at the U.S Southern Border as well as in the UAE and UK. Some of these deals occur via a subsidiary of Elbit Systems of America called Kollsman Inc, which is involved in a controversial death of an employee during a work trip to Saudi Arabia.

- These relationships are further strengthened through VC investments. The UAE invested at least $100 million in Israeli VC firms, which is not surprising, considering it is a longtime customer of its spyware tools. An Israeli owned company, for example, is behind Abu Dhabi's mass surveillance system, in a contract worth $600m. Dubai also operates a back-channel for Arab countries who wish to deploy Israeli surveillance technologies through a local entity called Black Wall Global, which is led by Israeli intelligence veterans.

- In similarly structured deals, Israeli companies like IntuView have contracts with Saudi Arabia for efforts that include scanning Saudi citizens' data. Its advisory board consists of a former head of Mossad and a former director of the CIA.

- The technology is becoming increasingly advanced and appealing to authoritarian governments. Israel, with the assistance of U.S companies, is deploying robots equipped with numerous sensors and cameras to surveil buildings and open spaces.

- AI-based systems like "The Gospel" largely consist of drone footage, intercepted communications, surveillance data and information drawn from monitoring the movements and behavior patterns of individuals and large groups to create bombing targets.

- In a similar setup, through "Lavender", Israel is using AI to detect assassination targets with little human oversight through information collected via mass surveillance of Gaza residents. The report highlights how many of these attacks result in the mass killing of civilians and entire families, often in their own homes.

- Spyware has always been a highly lucrative and increasingly prominent business in Israel. Citizen Lab has spent years uncovering sophisticated spyware from Israeli companies like NSO, which contracts with governments with a long history of imprisoning, murdering and silencing dissidents and surveilling civil society organizations, including Saudi Arabia, Bahrain and the UAE. These governments normalize relations with Israel largely to facilitate access to such technologies, which they then deploy to oppress their own citizens.

- Israel-based Voyager Labs actively marketed and sold surveillance tools which have been used to profile and intimidate journalists and activists, including by Colombian military intelligence. They recently moved their headquarters to the U.S. to continue building such tools with a team of "world-class AI researchers."

- U.S.-Israeli company Verint, whose products include surveillance cameras and analysis software to monitor and analyze large voice and video data sets, had sold their technology to repressive regimes in Azerbaijan, Indonesia, South Sudan, Uzbekistan and Kazakhstan. Among the uses of their tools is the violent crackdown on LGBTQ+ communities and human rights activists.

- These companies don't operate alone. When facing scrutiny or exposure, they spin off new entities, often with the backing of venture capital firms that are equally complicit. Verint, for example, spun off a separate company called Cognyte to continue its lucrative deals, which an Israeli human rights lawyer says was "aiding and abetting crimes against humanity." A New York-based hedge fund, Edenbrook Capital, is among its largest shareholders.

- Another and more recent example is Dream Security from the former CEO of Pegasus Software. Their latest round was raised in a deal that was co-led with Los Angeles-based VC firm Group 11. This demonstrates a troubling cycle of evasion.

- Corsight, an Israeli company, has been using facial recognition and Google Photos to conduct mass surveillance of Palestinians without their knowledge or consent. To date, Google has declined to answer, despite prohibiting their tech in being used for "immediate harm." Apart from being an egregious privacy violation, the technology also misidentifies people, putting their lives at risk. Canadian-Israeli VC firm, AWZ ventures, is among its lead investors. Their tools are also deployed by the U.S. Department of Homeland Security for facial recognition purposes.

- AnyVision, an Israeli company with an international presence, is behind "advanced tactical surveillance" software used to monitor the movements of Palestinians. Its CEO is a former

operating partner at SoftBank's investment arm, which co-led a large fundraising round for the company alongside Eldridge, an American holding company headquartered in Connecticut. A few months after the extent of their surveillance systems were exposed in U.S schools, they rebranded to Oosto and resumed operations.

- One of the most prominent examples of these collaborations remains Palantir, which also continues to win major contracts with the UK government and various U.S agencies, most recently the U.S army on an AI-powered targeting system, and who will once again supply its surveillance products to Israel in a new "strategic partnership."

- The global market for "Border Security Technologies" is projected to exceed $70 billion by 2027, up from $48 billion in 2022. The significant growth in this market is partly attributed to the increasing adoption of AI-integrated surveillance towers, made possible by Israeli companies who test repressive technologies on Palestinians. This practice allows Israel to refine and demonstrate the effectiveness of its products in real scenarios, making them more appealing to international buyers, who, again, are often equally oppressive regimes with horrific human rights records.

As shown above, these technologies, initially used to enforce violent occupation, apartheid, and genocide have found a lucrative global market, stretching far beyond the confines of Palestine. Antony Loewenstein, author of The Palestine Laboratory, notes to Tor: "Since 7 October, 2023, Israel has been live-testing new weapons in Gaza including drones, quadcopters, facial recognition tools and surveillance tech. The aim isn't just to kill Palestinians indiscriminately in Gaza but sell these weapons of war to a global market. AI-enabled warfare is a key selling point for the Israeli state and its private backers. What starts in Palestine never stays there."

Building a Culture of Accountability

The export of military systems by Israel reveals a harrowing journey of surveillance technologies from local deployments in Palestine to worldwide distribution, with a disturbing and alarming trend of normalization and acceptance of the grave human rights violations that are committed in the process of their creation and testing. The complicity of venture capital in the proliferation of such technologies highlights the intricate web of interests that prioritize power and profit over basic human rights.

This is your reminder that standing against surveillance that continues to engulf us all is a global responsibility. There needs to be a consistent and immediate call to action for tech workers, companies, civil society organizations, and the global community at large to stand firm in our commitment to human rights and privacy. We must hold companies accountable, dissect and expose the origins of surveillance technologies, and resist their normalization.

We applaud the companies and civil society organizations who have joined the No Tech For Apartheid campaign, including the many who risked their employment to do so, and urge others to join in this crucial effort. As many tech workers also have investment portfolios, we highly recommend that you align your investments with your values. This is one free screening tool you can use to ensure you're not profiting off of weapons manufacturers, illegal occupations, apartheid, genocide and border militarization, all of which use intense surveillance that enable the perpetration of war crimes.