Big Tech Complicity

ICE and Immigration Enforcement

Palantir Technologies Inc. is an American publicly traded company that develops data integration and analytics platforms enabling government agencies, militaries, and corporations to combine and analyze data from multiple sources. Its flagship products—Gotham (for intelligence and defense) and Foundry (for commercial and civil use)—connect previously siloed databases to support intelligence operations, counterterrorism analysis, law enforcement, and enterprise analytics.[3] Headquartered in Miami, Florida, it was founded in 2003 by Peter Thiel, Stephen Cohen, Joe Lonsdale, Alex Karp, and Nathan Gettings. According to a user guide obtained by 404 Media, a Palantir app "Enhanced Leads Identification & Targeting for Enforcement (ELITE), rolled out in late 2025, is a targeting tool designed to improve capabilities for identifying and prioritizing high-value targets through advanced analytics," the user guide states.

This software provides ICE agents with a digital map populated by potential deportation targets, each of which has their own detailed dossier, including information such as their name, date of birth, Alien Registration Number (a unique identifier assigned by the U.S. government), and a photograph of the target. The dossier also includes a "confidence score" out of 100 as to how certain the app is of the target's address. The information comes from a number of sources, including the Department of Health and Human Services, U.S. Citizenship and Immigration Services, and something called CLEAR, which could be an investigation software from Thomson Reuters, according to 404Media.

While the user guide does not explicitly state what company created the app, the app's full name appears in a $29.9 million supplemental agreement with Palantir that started in September and is planned to continue for at least a year, 404Media reported.

Palantir contracts with Immigration and Customs Enforcement (ICE) to track undocumented immigrants sparked outrage among privacy advocates and employees

https://en.wikipedia.org/wiki/Palantir

https://newrepublic.com/post/205333/ice-palantir-app-raid-deportation late 2025

Microsoft Azure
The *Guardian, +972 Magazine,* and *Local Call* found that ICE had tripled the amount of data it stored on Microsoft's Azure servers between July 2025 and January 2026, to an astounding 1,400 terabytes, and also appears to be using Microsoft's AI tools to search and analyze that data. This is the same Microsoft tech Israel uses to surveil and kill Palestinians. This led to the worker-led organization *No Azure for Apartheid.*

ICE is using the same Microsoft tech Israel uses to surveil and kill Palestinians. In just six months, Immigration and Customs Enforcement (ICE) more than tripled the amount of data stored on Microsoft's Azure cloud platform, *The Guardian* reports, "at the same time that its arsenal of surveillance technology ballooned." This week, tech workers with the No Azure for Apartheid (NOAA) campaign staged a protest and informational picket at Microsoft's global headquarters in Redmond, Washington, demanding that Microsoft cancel all contracts that provide technological support for Israel's ethnic cleansing of Palestinians and ICE's campaign of terror in the US.

https://therealnews.com/ice-is-using-the-same-microsoft-tech-israel-uses-to-surveil-and-kill-palestinians

February 26, 2026

9/11 Software: Made in the USA

PROMIS software

PROMIS software was created in the 1970s by former National Security Agency programmer and engineer Bill Hamilton, now president of Washington DC based Inslaw (Institute for Law and Social Research) Corporation. PROsecutor's Management Information System crossed a threshold in the evolution of computer programming. PROMIS was able to simultaneously read and integrate any number of different computer programs or databases simultaneously, Regardless of the language in which the original program had been written. Michael Ruppert, *Crossing the Rubicon* p 152-155. Reagan confident and overseer for domestic affairs from 1981 to 1985, Ed Meese loved PROMIS software. After a Series of demonstration showing how well PROMIS software could integrate the computers of dozens of us attorneys' Offices Around the country, the Department of Justice ordered the software to be installed under a highly controlled and limited license. Michael C Ruppert *Crossing the Rubicon*, 2004, p 152 f

From there however, Meese and his cronies allegedly modified it to include a backdoor that would allow those who knew of it to access the program in other computers. The PROMIS managed data could be anything from financial records to tracking movement of people. That made the program a natural for Israel that, according to Hamilton and many other sources, was one of the first countries to acquire the bootlegged software from Meese. Michael Ruppert, *Crossing the Rubicon* p. 156

Confidential documents obtained by Ruppert's *From The Wilderness* indicate that much of the AI development was done at the Los Alamos National Laboratory and Sandia labs using research from other US universities, Including Harvard, Caltech, and the University of California. PROMIS came to life years before the election of Ronald Reagan. It was also according to Ruppert informant Bill Tyree an essential element in the espionage conducted by Jonathan Pollard against not only the US government, but the Washington embassies of many nations targeted by Israelis' Mossad.

Evidence has surfaced that the famous Mossad spy Rafi Eitan obtained a copy of this software. As described by Inslaw attorney, the late Elliot Richardson, the Israeli Mossad under Eitan's direction,

with the aid of Robert Maxwell, planted another backdoor in PROMIS, and sold it to governments of some 40 countries throughout the world. Every time this software is used, Israeli intelligence can see everything that is done.

https://thewashingtonstandard.com/mega-group-maxwells-and-mossad-the-spy-story-at-the-heart-of-the-jeffrey-epstein-scandal/

https://www.muckrock.com/news/archives/2017/oct/12/promis-israel

PTech

Just because software is “made” in the US, that doesn’t mean it is necessarily made by the US. PTech is important to an understanding of US government failures on 9/11/2001.

Indira Singh on PTech and 9/11

The following is from the Oct 14, 2011 episode 045 of the Corbett Report, titled *Ptech and the 9/11 Software*. This in turn provides a transcript of Bonnie Faulkner’s in depth 2005 interview with Indira Singh on the program “Guns and Butter”.

Webster Tarpley has identified 26 wargames taking place on or around, 9/11 that directly affected the U.S. Air Force’s ability to counteract the hijackings that day.

https://corbettreport.com/episode-020-webster-tarpley-on-the-911-drills/

Indira Singh was hired as a consultant for J.P. Morgan-Chase to develop the next generation of business architecture enterprise software. The importance, sensitivity, and sophistication of any such software necessarily led Ms. Singh to seek out the true leaders in the enterprise architecture software industry. Her research and due diligence into the issue led her to a company called PTech, a Quincy, Massachusetts-based provider of business process modeling software whose clients included many federal governmental agencies, including the U.S. Army, the U.S. Air Force, the U.S. Naval Air Command, Congress, the Department of Energy, the Federal Aviation Administration, the Internal Revenue Service, NATO, the Federal Bureau of Investigation, the Secret Service and even the White House.

It was subsequently revealed that their financier, their funders, their investors were all Saudis, and she found that the chief investor, Sheikh Yassin al-Qadi, was placed on the U.S. terror list on October 12, 2001. The FBI was notified of this but refused to take any action. “The agent said the FBI would not proceed [with any investigation], but sent her a video tape. The substance of the video tape was a news clip of a CBS affiliate based in Boston, called WBZ-TV. Their investigative reporting team – the I-Team – which was led by investigative reporter, Joe Bergantino, had investigated a number of Middle Eastern men who were sought after 9/11. They were affiliated with Muslim-Islamic terrorism financing charities. He had created this clip to show the connection between the 9/11 terror attack and the financial vehicles that were supposedly used to fund it. The I-Team connected something called “Care International” – that was based in Boston all the way back to al-Keefah which was the financing vehicle at the center of the World Trade Center bombing in 1993; all the way back to something called Maktab al-qeedah mad, which means “the office”, which was a financing vehicle that was set up by the CIA for the Pakistani ISI back in the days when Osama Bin Laden was America’s fair-haired boy and was on our side fighting with the Mujahidin, fighting the Soviet Union….

when I was finished with certain parts of the investigation, it was clear to me that there was no way PTech could have done all of this without a lot of inside help. That is what I began focusing on: that it was a cutout, that it was a front. Was it a regular CIA front? Was it a clandestine front? What was it? There are walls within the FBI, walls within the CIA, behind which these operations take place. Who is behind those operations is a key question.

Bonnie: Could you describe the relationship of PTech with the FAA? PTech worked with the FAA for several years, didn't they?

Indira: Yes. It was a joint project between PTech and MITRE. It is interesting. They were looking at, basically, holes in the FAA's interoperability with responding with other agencies – law enforcement – in the case of an emergency such as a hijacking.

Bonnie: Was there a reference to PTech having operated in the basement out of the FAA?

Indira: Yes. Typically, because the scope of such projects are so over-arching and wide-ranging, when you are doing an enterprise architecture project, you have access to how anything in the organization is being done, where it is being done, on what systems, what the information is. You have carte blanche.

If it is a major project that spends several years, the team that comes in has, literally, access to almost anything that they want because you are operating on a blueprint level, on a massive scale. So, yes, they were everywhere, and I was told that they were in places that required clearances. I was told that they had log-on access to FAA flight control computers. I was told that they had passwords to many computers that you may not, on the surface, think has anything to do with finding out holes in the system…

…in the White House, Ari Fleischer, spun it to fine sugar that day. He said there's nothing wrong; nothing here; not a thing to see here; everything is fine.

They did a token raid and that was basically it.

….

Indira: It is possible that there was an alternate command and control system. Could you technically use PTech software to do surveillance and intervention? Well, gosh, yes. That is exactly what I was planning on using it for in one of the largest banks in the world. It is not a problem….However, I cannot say for sure that that was going on because I do not have direct first-hand knowledge of that and no one has told me and offered me proof of that. But could I state that it could happen? Absolutely, it could have happened.

Bonnie: What happened with the raid that the FBI staged on P-Tech?

Indira: Well, what happened was, when I took all of this information back to JPMorgan, after agent Wright had appeared on the steps of the Capitol, then I went down to Virginia, I got all the information together. I had the P-Tech people actually write it out, so it wouldn't be, 'Indira says', it would be, 'this is what they put together'. And I had emails, documentation, photographs, photographs that flew around the world, that were plastered all over network TV, that's what I got from these people and I interviewed a bunch of scared people, "What is going on? The FBI knows about it and they're doing nothing… What is going on? What do you think this tells you?" And I didn't wanna go there without proof, I wasn't gonna go there. Really what I did, and the most powerful thing, I think, anyone can do, is not just to make an accusation or get a little bit of proof which can be hushed up and denied, but I

took what I had to everyone. Before P-Tech was ever raided, before it ever became public, I took it all the way up to the top of the FBI, I took it everywhere.

And the reality of the situation is proven by the response I got there… More telling than the actual deed itself. Their response to that is really what indicts them all.

Bonnie: What was their response?

Indira: Uhm, “Shut up and go away, or you will be killed!” Basically…

Bonnie; Now, you got that response from all different levels in government…

Indira: I got that response from JPMorgan. I got that response from P-Tech. I got that warning from people within the FBI. Mostly the FBI.

”See, when the Boston FBI sent me that tape that Joe Bergantino had run the story on, I looked at the tape and it was all P-Tech people… I was really scared. And I contacted Joe Bergantino to tell him I’ve been threatened, people had been in my house, I’m a 9/11 survivor, I can’t back down on this, and if anything happens to me, the story that you did… did you know that these people worked at P-Tech? He said, “We had some suspicion, we didn’t know.” And I said, “Well let me tell you what P-Tech does…” When I went out there and I spoke to them in June, 2002, they thought I had a flowerpot growing out of my head. They didn’t believe me at all. I said, “You’ve done the original story, you just don’t realize that they’re connected to corporate America and the government in this way…”

“So what they did is they initiated their own investigation, and their own investigation, they came back to me and said, “We’re sorry for having doubted you, it’s not only as bad as you said, it’s much, much worse.” This is a CBS affiliate by the way… and they had interviewed me and taped me and this is August, 2002, they had said, “We’re going to run this story on the one-year anniversary of 9/11.” And I was horrified, I begged them I said, “Please do not delay, get it out now.” And they said, “No, it’s not gonna play well in August, because everyone’s on vacation…” And I was banging my head against the wall, I was in tears. And I said, “They’re gonna shut this down. People are gonna talk, they’re gonna find out about it and shut you down.” And sure enough, they did. … 7 networks … caught wind of this story, and they shut down the investigation.

“Absolutely, but they’ve renamed themselves, they’re called ‘Go Agile’ and they’re still going… Nothing… When we try to find out what the status of the investigation is, we’ve been told alternatively that they’ve been cleared or it’s still in limbo.

https://not2belost.wordpress.com/2017/01/12/21/

More on Indira Singh

on PTech and 9/11: Corbett Report:

https://www.seattle911visibilityproject.in/911VP_2025_update/wtcs/Singh-PTech-Cor.pdf

For some Indira Singh interviews, see:

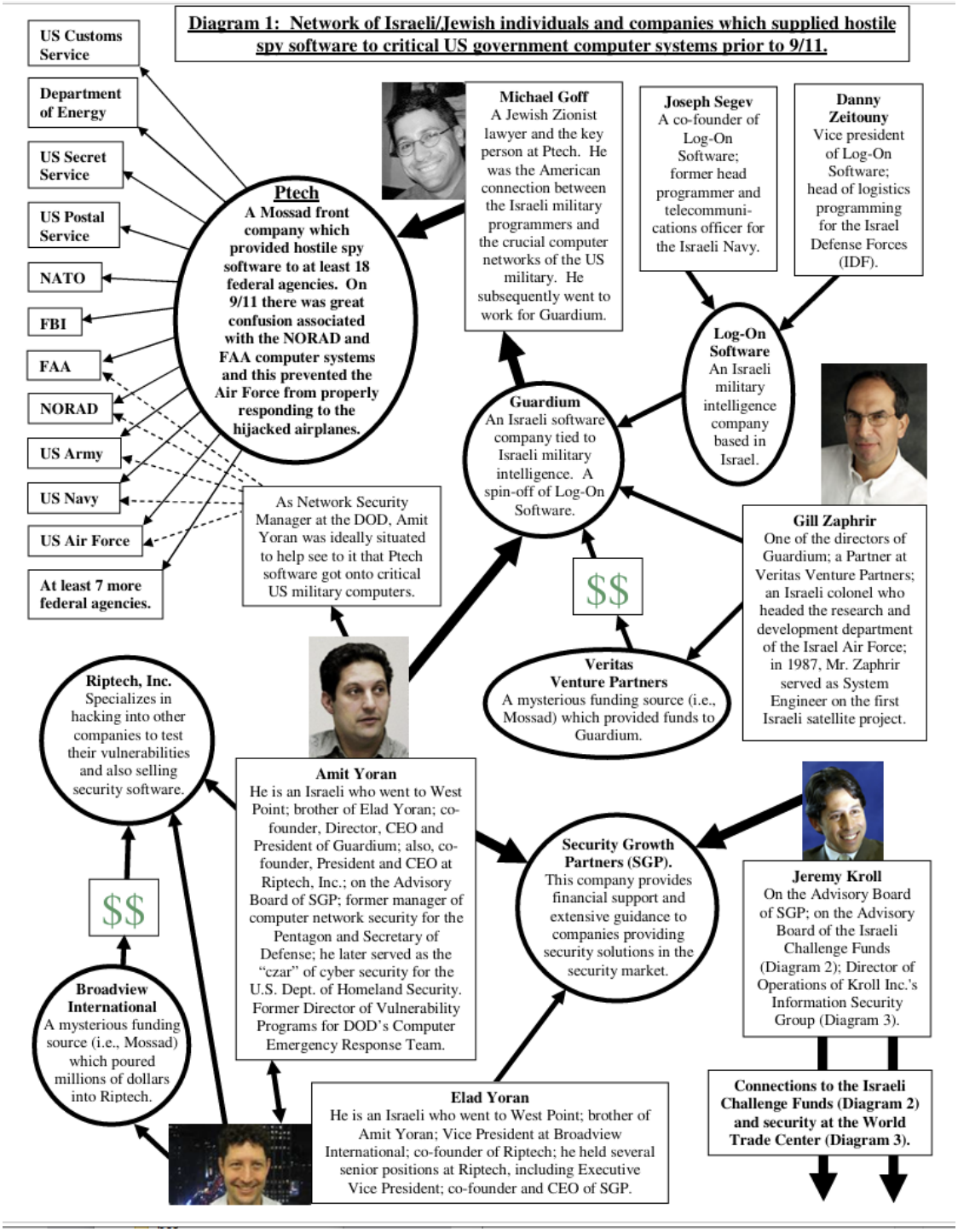
https://corbettreport.com/ptech-and-the-911-software/

https://not2belost.wordpress.com/2017/01/12/21/ 2017

https://archives.kpfa.org/data/20050427-Wed1400.mp3

https://archives.kpfa.org/data/20050720-Wed1400.mp3

Christopher Bollyn on Ptech



https://www.scribd.com/document/341810116/Ptech-diagram-pdf

https://www.bollyn.com/public/Ptech_and_Computer_Network.pdf

Mike Ruppert: From the Wilderness


FromTheWilderness.com
mirror site
WWW.COPVCIA.COM
Become a member! Click here to visit the FTW Online Store!
PTECH, 9/11, and USA-SAUDI TERROR - Part I
PROMIS Connections to Cheney Control of 9/11 Attacks Confirmed
by
Jamey Hecht
With research assistance by Michael Kane and editorial comment by Michael C. Ruppert

"I believe that Dick Cheney also had the ability using evolutions ofhe PROMIS software, to penetrate and override any other radar computer or communications system in the government."

- Mike Ruppert, in "Summation: Ladies and Gentlemen of the Jury," from *Crossing The Rubicon,* p.592

PTECH-911-USA-SAUDI-TERROR-Part1.pdf renamed to: PTECH-RUPPERT:

https://www.seattle911visibilityproject.in/911VP_2025_update/wtcs/PTECH-RUPPERT.pdf

Indira Singh and PTech From the Wilderness Website Timeline:

https://www.seattle911visibilityproject.in/911VP_2025_update/wtcs/Timeline from Michael Ruppert.pdf

Israeli Designed Software

NSO Group-Pegasus

The Israeli firm NSO Group sparked outrage in 2021 after an investigation by international media outlets revealed that its Pegasus spyware was used by security forces and authoritarian governments against journalists and activists in several countries. NSO says it works with law enforcement agencies to track criminals and “terrorists.” The phones of at least nine US State Department employees were also hacked using this same spyware. The hacking targeted the Apple-made iPhones of US officials based in Uganda or working on issues related to the country.

https://www.aljazeera.com/news/2021/12/3/us-officials-phones-hacked-nso-group-spyware-reuters 3 December 2021

Israeli surveillance company Paragon Solutions tried to position itself as the “ethical” alternative. Paragon’s flagship product, Graphite, represents the cutting edge of what researchers call “mercenary spyware”— highly targeted intrusion systems sold exclusively to state agencies. Paragon’s founding team includes the former Israeli PM Ehud Barak, as well as former Unit 8200 commander Ehud Schneorson, exposing how Israeli intelligence expertise metastasizes into private markets. The same skills used to monitor Palestinians in the occupied territories are now being sold to governments worldwide

The Israeli army has marked tens of thousands of Gazans as suspects for assassination, using an AI targeting system designated as "Lavender", with little human oversight and a permissive policy for casualties. According to six Israeli intelligence officers, who have all served in the army during the current war on the Gaza Strip and had first-hand involvement with the use of AI to generate targets for assassination, Lavender has played a central role in the unprecedented bombing of Palestinians, especially during the early stages of the war.

Paragon Solutions- Graphite

Israeli surveillance company Paragon Solutions tried to position itself as the “ethical” alternative. Paragon’s flagship product, Graphite, represents the cutting edge of what researchers call “mercenary spyware”— highly targeted intrusion systems sold exclusively to state agencies.

Paragon Solutions briefly exposed its own spyware dashboard on LinkedIn, revealing the hidden architecture of a billion-dollar surveillance empire built on the backs of journalists, activists, and ordinary people. This technical slip-up is a moment of rare transparency in an industry built on secrecy, exposing the operational interface used to compromise devices, intercept communications, and harvest data from targets worldwide.

The $900 million acquisition of Paragon by U.S. private equity firm AE Industrial Partners tells you everything you need to know about who profits from your digital insecurity. Former Israeli Prime Minister Ehud Barak reportedly pocketed $10-15 million from the deal, a tidy sum for a politician-turned-surveillance capitalist. Paragon’s founding team also includes former Unit 8200 commander Ehud Schneorson.

Carbyne

Ehud Barak helped Jeffrey Epstein quietly invest $1 million in a tech startup Reporty, later renamed Carbyne, in 2015. According to recently released Department of Justice emails, Barak was an early investor and the board chairman of Reporty.

https://www.forbes.com/sites/thomasbrewster/2026/02/10/epstein-police-surveillance-investments-with-ehud-barak

Developed by former members of Israel's elite spy units, Carbyne's tech is designed for emergency responders. When a 911 call comes in, the software allows the caller to use their smartphone camera to stream video to police HQ so officers can see what is happening on the ground.

Toka

Barak also sought Epstein's help with Tel Aviv based surveillance business Toka, just before Barak publicly launched it in July 2018 with $12.5 million in funding from the likes of Andreessen Horowitz.

These examples show how Israeli intelligence expertise metastasizes into private markets. The same skills used to monitor Palestinians in the occupied territories are now being sold to governments worldwide.

Israeli- made Pegasus spyware has been licensed to roughly 45 governments worldwide, including at least 5 to 14 European Union states,

Paragon's flagship product, Graphite provides "precision intrusion for the 1%", and represents the cutting edge of what researchers call "mercenary spyware"— highly targeted intrusion systems sold exclusively to state agencies. Unlike conventional malware, these platforms are engineered for precision, using zero-click exploit chains that compromise devices without any action from the target.

Once installed, spyware operates at the operating-system level, granting operators visibility into stored data and communications, microphone and camera activation, enclosed applications and services, and messages accessed before encryption or after decryption.

https://ahmedeldin.substack.com/p/the-israeli-spyware-firm-that-accidentally

Lavender AI

The Israeli army has marked tens of thousands of Gazans as suspects for assassination, using an AI targeting system with little human oversight and a permissive policy for casualties.

In 2021, a book titled *The Human-Machine Team: How to Create Synergy Between Human and Artificial Intelligence That Will Revolutionize Our World* was released in English under the pen name "Brigadier General Y.S." In it, the author — a man who we confirmed to be a commander of the elite Israeli intelligence unit 8200 — makes the case for designing a special machine that could rapidly process massive amounts of data to generate thousands of potential "targets" for military strikes in the heat of a war. Such technology, he writes, would resolve what he described as a "human bottleneck for both locating the new targets and decision-making to approve the targets."

Such a machine, it turns out, actually exists. A new investigation by *+972 Magazine* and *Local Call* reveals that the Israeli army has developed an artificial intelligence-based program known as "Lavender." According to six Israeli intelligence officers, who have all served in the army during the current war on the Gaza Strip and had first-hand involvement with the use of AI to generate targets for assassination, Lavender has played a central role in the unprecedented bombing of Palestinians, especially during the early stages of the war.

https://www.972mag.com/lavender-ai-israeli-army-gaza/ April 3 2024

Palantir and Israel

Palantir also supports Israel with predictive surveillance and national security tools. The collaboration between Palantir and Israel's Ministry of Defense officially began in July 2023, with the company signing a formal contract to supply its AI-powered software specifically for military applications. This agreement came just months before the October 7th conflict escalation, positioning Palantir's technology at the center of Israel's defense infrastructure. US Palantir and Israeli Lavender AI systems have overlapping capabilities in data analysis and target identification algorithms.

This conflicts with claims that the Palantir AI system is somehow "different" than Lavender: "Palantir's systems, while also used by military and intelligence bodies, are products of a commercial company that collaborates with multiple international organizations. This gives Palantir "a broader scope."

https://ithy.com/article/military-ai-analysis-de66660s

Yes, this means Palantir's AI could be used in a similar way that Lavender is. Also, considering the benefit brought to Israel by Palantir in 2023, Lavender's independence from Palantir is still a subject of debate. Alex Karp, Palantir's CEO, has been vocal about the company's alignment with Israel's military objectives. In multiple public statements, Karp expressed unwavering support for Israel's operational priorities.

According to documents revealed by Edward Snowden, the US National Security Agency has long been a key intelligence provider to Israel. This partnership operates under a Top Secret/Special

Intelligence agreement between the NSA and Israel's SIGINT National Unit (ISNU). Critical intelligence from NSA continues to flow to Unit 8200, Israel's elite intelligence agency, which then feeds this data into Palantir's systems. Internal dissent at Palantir has escalated as employees grapple with the ethical implications of the company's work. CEO Alex Karp openly acknowledged losing staff over Palantir's support for Israel.

August 4 2025 https://decodingaffairs.com/israel-palestine-conflict/boycott/palantir-supports-israel/
https://en.globes.co.il/en/article-What-is-Palantir-doing-in-Israel-1001468876
More Information on Palantir

Israeli Support for International Conflict

In this two-part series, Al Jazeera English's "The Palestine Laboratory" film, journalist Antony Loewenstein investigates how Israeli weapons and surveillance technologies are first used to control and repress Palestinians in Palestine before being sold all over the world.

In episode one, in Israel and Palestine, the film examines how Israel positions itself as a world leader in hi-tech weapons and surveillance technology, with glossy promotions from the top weapons manufacturers boasting that their products have been "tested" and "proven" in "battle". Hearing from both Israelis and Palestinians, the film explores how the arms industry understands what labels like "tested" in Palestine mean and how the military intelligence Unit 8200 acts as an incubator for Israeli surveillance tech start-ups. In addition, it examines Israel's use of AI targeting systems in Gaza.

Episode two of the investigation takes Loewenstein on an international journey to reveal how this "technology of occupation" is used to subjugate and surveil political dissidents, human rights activists and journalists all over the world, and how this surveillance and military technology developed by Israel and tested on Palestinians is marketed abroad. It reveals how the latest Israeli technology is being used to monitor refugees and migrants in Greece and along the US-Mexico border.

Loewenstein visits Mexico to explore its use of Israeli spyware and travels to India to discover how a thriving arms trade fosters close links between the two nations. In South Africa, he uncovers a hidden aspect of the country's history which saw a secret relationship between the apartheid-era government and Israel, centered on a clandestine arms trade and shared values.

https://www.youtube.com/watch?v=1GvkFwpzDhI

Description:

https://network.aljazeera.net/en/press-releases/%E2%80%98-palestine-laboratory%E2%80%99-exposes-israel%E2%80%99s-export-unique-systems-control-and

US Economic and Technical Support for Israeli Genocide

Probes Reveal Depth of Big Tech Complicity in Israel's AI-Driven Gaza Slaughter

"Many nations are looking to Israel and its use of AI in Gaza with admiration and jealousy," said one expert. "Expect to see a form of Google, Microsoft, and Amazon-backed AI in other war zones soon."

Several recent journalistic investigations—including one published Tuesday by *The Associated Press*—have deepened the understanding of how Israeli forces are using artificial intelligence and cloud computing systems sold by U.S. tech titans for the mass surveillance and killing of Palestinians in Gaza. …The *Associated Press* found that Israel's use of Microsoft and OpenAI technology "skyrocketed" following Hamas' October 7, 2023 attack on Israel. … "This is the first confirmation we have gotten that commercial AI models are directly being used in warfare," Heidy Khlaaf, chief artificial intelligence scientist at the *AI Now Institute* and a former senior safety engineer at OpenAI, which makes ChatGPT, told the *AP*. "The implications are enormous for the role of tech in enabling this type of unethical and unlawful warfare going forward."

https://www.commondreams.org/news/big-tech-gaza-genocide Feb 18, 2025

Notably, technology companies in Israel represent a significant economic force, housing 10% of the world's unicorns and contributing 20% of the country's GDP. [A tech unicorn is a company that has been valued by investors at more than one billion dollars.] The relationship between Israeli tech companies and American investors is particularly strong, with U.S.-based investors leading or co-leading 51% of the $32 billion invested in Israeli companies since 2019. This investment is not necessarily known by investors, and it is difficult to avoid. Major US fiduciary businesses, such as Vanguard, are complicit. Although Israeli software is not necessarily used for genocide, its profits are.

US Tech Companies that support Israel's Genocide have played a far more significant role in the ongoing conflict than many realize. In the aftermath of October 7, 2023, major US technology companies have demonstrated their support for Israel through various actions, statements, and business decisions. Tech executives quickly took public positions. Google CEO Sundar Pichai condemned the Hamas attacks as "terrorism," whereas Meta's Mark Zuckerberg expressed his support by stating that "Israel has every right to defend itself." However, these statements came alongside selective content moderation policies on their platforms.

Many US tech leaders remained strategically silent about the civilian casualties in Gaza. This contrasts sharply with their vocal responses to other global conflicts, such as the Russia-Ukraine war. This selective approach to humanitarian concerns has drawn criticism from both employees and human rights observers.

Tech company positions mirror broader US foreign policy objectives in the Middle East. Government contracts often incentivize private sector alignment with strategic allies. For instance, defense-related

technology development receives significant funding through initiatives that connect Silicon Valley with Israel's military-industrial complex. The revolving door between government positions and tech leadership roles further cements this relationship. Former government officials frequently transition to executive positions at technology companies, bringing established policy perspectives with them. Consequently, corporate decision-making often aligns with long-standing US foreign policy positions.

Google and Alphabet: Providing cloud services through Project Nimbus and expanding research facilities in Tel Aviv.

Google Photos

Google Won't Say Anything About Israel Using Its Photo Software to Create Gaza "Hit List" - The Intercept.pdf" Google prohibits using its tech for "immediate harm," but Israel is harnessing its facial recognition to set up a dragnet of Palestinians. The Israeli military has reportedly implemented a facial recognition dragnet across the Gaza Strip, scanning ordinary Palestinians as they move throughout the ravaged territory, attempting to flee the ongoing bombardment and seeking sustenance for their families.

The program relies on two different facial recognition tools, according to the New York Times: one made by the Israeli contractor Corsight, and the other built into the popular consumer image organization platform offered through **Google Photos**. An anonymous Israeli official told the Times that Google Photos worked better than any of the alternative facial recognition tech, helping the Israelis make a "hit list" of alleged Hamas fighters who participated in the October 7 attack.

https://theintercept.com/2024/04/05/google-photos-israel-gaza-facial-recognition/ April 5 2024,

https://www.nytimes.com/2024/03/27/technology/israel-facial-recognition-gaza.html

Amazon Web Services: Major cloud infrastructure provider to Israeli government entities.

Project Nimbus – a $1.2 billion agreement where Google and Amazon provide cloud computing services to the Israeli government and military.

Amazon and Google have expanded their physical presence through data centers and research facilities.

Microsoft: Supplying Azure cloud technology and AI tools to Israeli defense forces .

Microsoft has increased its stake in the Israeli AI industry, acquiring several startups in recent years.

Meta (Facebook): Content moderation policies favoring pro-Israel perspectives.

IBM:

After the attacks of 9/11/2001, Indira Singh, working for J.P. Morgan-Chase, contacted her representative at IBM, Kyle Hiligoss. She suggested that before IBM get seriously involved with PTech, they do some background checking. "Kyle told me that he 'wrote a book report' and sent it to his legal department. He was told to just back off the whole thing. In fact, he did not even want to have anything to do with me as I continued investigating."

The roots of IBM's involvement in Israel date back to 1972, with the establishment of the **IBM Israel Scientific Center**. Presently, IBM boasts over 1000 employees spread across various Israeli

locations, notably in Haifa, Tel Aviv, Herzliya, Rehovot, and the Jerusalem Technology Park. IBM Provides biometric identification systems and database technologies. It designed and now operates the Eitan System for Israel's Population, Immigration and Border Authority, storing personal information on Palestinians. This biometric database documents and controls Palestinian movement at checkpoints while managing permits needed for work, medical care, and family reunification. In 2017, IBM won a $240 million contract to design this system, assuming full responsibility for Israel's population registry by 2019. Importantly, Norwegian asset management company Storebrand recently divested approximately $139 million from IBM, stating the company's biometric database "contributes to discrimination and segregation of Palestinians".

Oracle: Extensive data management services to Israeli government agencies.

Palantir: Offering predictive analytics capabilities for security applications.

Cellebrite: Developing phone data extraction technologies used by authorities: Cellebrite and phone data extraction from detainees.

Israeli firm Cellebrite provides phone-cracking technology that extracts comprehensive data from seized devices without requiring passwords. Their systems can download messages, calls, images, location history, and even recently deleted content from detained individuals' phones.

https://www.commondreams.org/news/2021/09/10/big-tech-war-profiteers-raked-44-billion-during-global-war-terror

Anthropic's Claude AI being used in Iran war by U.S. military, sources say

March 3 2026

Two sources fa liar with the U.S. military's use of artificial intelligence confirm that the U.S. used Anthropic's Claude AI model over weekend for the attack on Iran — and is still using it. …It's being used despite a government-wide ban on the technology announced after an Anthropic dispute with the Pentagon. The conflict centered around Anthropic's push for guardrails that would explicitly prevent the military from using Claude to conduct mass surveillance on Americans or to power fully autonomous weapons. Its use in the I ran war was first reported by the Wall Street Journal.It's unclear if the Israeli army is also using Claude during this conflict. An IDF spokesperson did not respond to CBS News' request for comment. The IDF does use AI in conducting warfare and has its own "Lavender" targeting system, which it used in the Gaza war.

https://www.cbsnews.com/news/anthropic-claude-ai-iran-war-u-s/

CENSORSHIP

Meta
Human rights watch report: Meta's policies and practices have been silencing voices in support of Palestine and Palestinian human rights on Instagram and Facebook in a wave of heightened censorship of social media amid the hostilities between Israeli forces and Palestinian armed groups that began on October 7, 2023. This systemic online Between October and November 2023, Human Rights Watch documented over 1,050 takedowns and other suppression of content Instagram and

Facebook that had been posted by Palestinians and their supporters, including about human rights abuses …In reviewing the evidence and context associated with each reported case, Human Rights Watch identified six key patterns of undue censorship, each recurring at least 100 times,

Palestinian civil society organizations condemn the selection of Emi Palmor, the former General Director of the Israeli Ministry of Justice, to Facebook's Oversight Board and raises the alarm about the impact that her role will play in further shrinking the space for freedom of expression online and the protection of human rights. Under Palmor's direction, the Israeli Ministry of Justice petitioned Facebook to censor legitimate speech of human rights defenders and journalists because it was deemed politically undesirable. This is contrary to international human rights law standards and recommendations issued by the United Nations (UN) Special Rapporteur...

During Palmor's time at the Israeli Ministry of Justice (2014-2019), the Ministry established the Israeli Cyber Unit, or 'Internet Referral Unit,' whose work has deliberately targeted and resulted in the takedowns of tens of thousands of Palestinians' content, and imposed severe limitations on freedom of expression and opinion, especially about Palestine...
At the same time, research into incitement to racial hatred against Palestinians online has shown that there were inciting posts in Hebrew directed towards Palestinians online every 66 seconds in 2018, while no interest was shown in combating such racist content against Palestinian Arabs.

Additionally, as documented in Facebook's Transparency Report, since 2016, there has been an increase in the number of Israeli government requests for data, which now total over 700. These fall within the context of a widespread and systematic attmept by the Israeli government, particularly through the Cyber Unit formerly headed by Emi Palmor, to silence Palestinians, to remove social media content critical of Israeli policies and practices and to smear and delegitimize human rights defenders, activists and organizations seeking to challenge Israeli rights abuses against the Palestinian people.

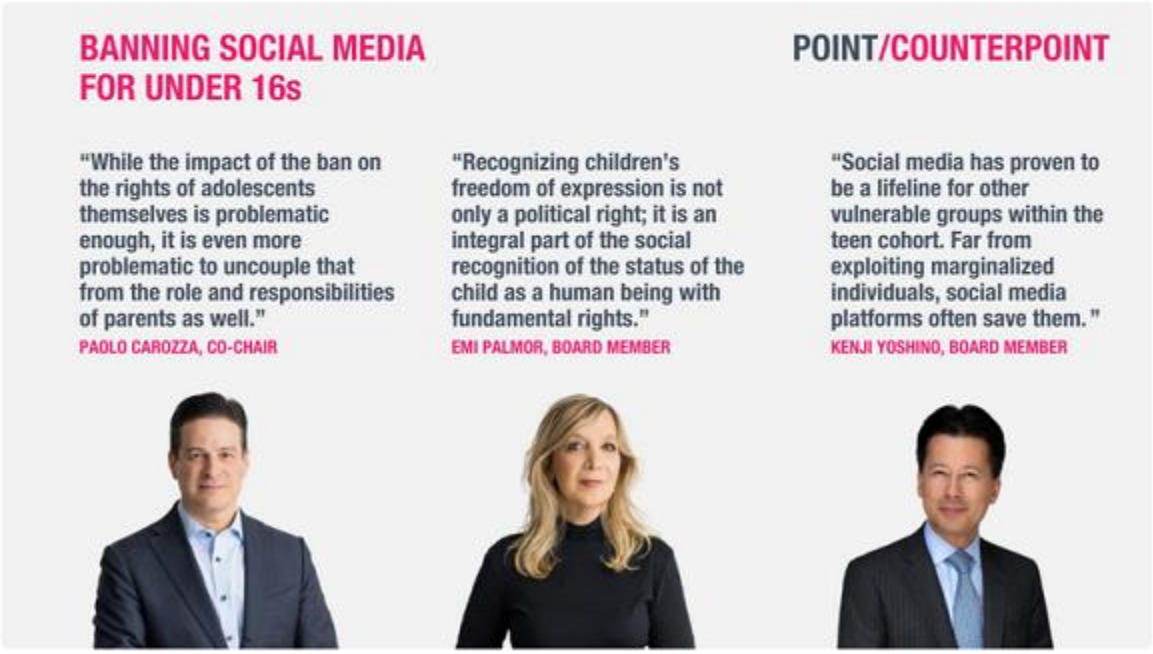
https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and
12/21/2023

Facebook/Meta Oversight Board links

https://www.oversightboard.com

https://www.oversightboard.com/news/social-media-bans-for-under-16-users-good-policy-wasted-effort-something-in-between

The Oversight Board is committed to upholding human rights online for all users. Our global Board Members represent a diversity of backgrounds, opinions and ideologies but share a commitment to protecting freedom of expression. Major social media companies have determined that children under 13 should not be on their platforms, while at the same time countries around the world consider following Australia's policy decision to ban young people under age 16 from social media entirely. Three of our Board Members share their perspectives on what's at stake, including for the 13 to 15-year-olds at the heart of the debate.



Tech Worker Revolts

No Tech for Apartheid campaign No Tech for Apartheid emerged as a worker-led movement against Project Nimbus.

https://decodingaffairs.com/israel-palestine-conflict/boycott/tech-companies-that-support-israel/

June 14 2025

no-tech-for-apartheid.pdf

https://www.notechforapartheid.com/

Microsoft's ties with ICE come under fire amidst allegations that the company's cloud and AI technology are being used to support mass surveillance of US citizens
No Azure for Apartheid, a worker-led organization that's previously carried out multiple protests over Microsoft's dealing with the Israeli military and its campaign in Gaza, has issued a statement calling on the company to end its relationship with US Immigration and Customs Enforcement, the agency more commonly known as ICE.

The statement follows reporting by The Guardian, +972 Magazine, and Local Call that found ICE had tripled the amount of data it stored on Microsoft's Azure servers between July 2025 and January 2026, to an astounding 1,400 terabytes, and also appears to be using Microsoft's AI tools to search and analyze that data.
https://www.yahoo.com/news/articles/microsofts-ties-ice-come-under-202655045.html

February 18, 2026

No Azure For Apartheid

argues the Microsoft tech "powers ICE's violence towards migrants and communities in the United States" In the aftermath of reports claiming that the US Immigration and Customs Enforcement agency (ICE) deepened their reliance on Microsoft’s cloud technology last year, No Azure for Apartheid have issued a statement demanding the company cut ties with the agency.

https://www.rockpapershotgun.com/no-azure-for-apartheid-call-on-microsoft-to-cut-ties-with-ice-amid-reports-of-agency-deepening-reliance-on-companys-cloud-and-ai

Published on Feb. 19, 2026

Time Exclusive google workers revolt over $1.2 billion israel contract

In midtown Manhattan on March 4, Google’s managing director for Israel, Barak Regev, was addressing a conference promoting the Israeli tech industry when a member of the audience stood up in protest. “I am a Google Cloud software engineer, and I refuse to build technology that powers genocide, apartheid, or surveillance,” shouted the protester, wearing an orange t-shirt emblazoned with a white Google logo. “No tech for apartheid!” The Google worker, a 23-year-old software engineer named Eddie Hatfield, was booed by the audience and quickly bundled out of the room. Hatfield is part of a growing movement inside Google that is calling on the company to drop Project Nimbus, a $1.2 billion contract with Israel, jointly held with Amazon. The protest group, called No Tech for Apartheid, now has more than 200 Google employees closely involved in organizing, according to members, who say there are hundreds more workers sympathetic to their goals.
https://time.com/6964364/exclusive-no-tech-for-apartheid-google-workers-protest-project-nimbus-1-2-billion-contract-with-israel/ Apr 10, 2024

Google Workers Protest Cloud Contract With Israel's Government

Google Workers Protest “Project Nimbus”, a joint Google Amazon cloud contract with Israel's government to store vast amounts of data has come under intense protest by Google employees, resulting in the firing of over 50. The firings come several days after chief executive Sundar Pichai told employees in a companywide memo that they should not use the company as a “personal platform” or “fight over disruptive issues or debate politics.” Dozens of Google employees began occupying company offices in New York City and Sunnyvale, California, in protest of the company’s $1.2 billion contract providing cloud computing services to the Israeli government. The sit-in, organized by the activist group No Tech for Apartheid, is happening at Google Cloud CEO Thomas Kurian’s office in Sunnyvale and the 10th floor commons of Google’s New York office. The sit-in will

be accompanied by outdoor protests at Google offices in New York, Sunnyvale, San Francisco, and Seattle. These actions mark an escalation in a series of recent protests organized by tech workers who oppose their employer's relationship with the Israeli government, especially in light of Israel's ongoing assault on Gaza.

https://www.wired.com/story/google-no-tech-for-apartheid-project-nimbus-israel-gaza-protest/ April 16 2024

About a dozen demonstrators lay on the ground draped in white sheets with a mock version of the Google logo, demanding an end to the company's work with the Israeli government, in San Francisco on Dec. 14,

Google fires more workers after CEO says workplace isn't for politics.

Washington post

SAN FRANCISCO — Google fired about 20 more workers whom it said participated in protests denouncing the company's cloud computing deal with the Israeli government, bringing the total number of workers week over the issue to more than 50, according to the activist group representing the workers. fired in the past A spokesperson for Google confirmed it had fired more workers after continuing its investigation into the April 16 protests, which included sit-ins at Google's offices in New York City and Sunnyvale, Calif. The firings come several days after chief executive Sundar Pichai told employees in a companywide memo that they should not use the company as a "personal platform" or "fight over disruptive issues or debate politics." "The corporation is attempting to quash dissent, silence its workers and reassert its power over them," said Jane Chung, a spokesperson for No Tech

for Apartheid, a group that has protested Google’s and Amazon’s contracts with the Israeli government since 2021.

https://www.washingtonpost.com/technology/2024/04/22/google-nimbus-israel-protest-fired-workers/

April 22, 2024