

Infrastructure for a Genocide: Big Tech's Role in the Gaza Extermination Campaign

Douglas C. Youvan

doug@youvan.com

www.youvan.ai

September 27, 2025

The genocide in Gaza is not unfolding in darkness — it is being illuminated, calculated, and accelerated by some of the most powerful technology companies on Earth. Microsoft, Amazon, Google, and OpenAI have provided AI models, cloud infrastructure, and computational services to the Israeli military throughout the ongoing extermination of Palestinians. As bombs fall on hospitals and refugee camps, these firms' platforms silently process vast volumes of surveillance data, enable AI-assisted targeting, and help orchestrate one of the most devastating assaults on a civilian population in modern memory. This paper examines the direct and indirect roles of these companies in what the UN and numerous human rights organizations now openly call a genocide. We trace the supply chains of digital war: the software licenses, the cloud contracts, the API access, and the political shielding. We also assess the corporate strategies of denial, partial disengagement, or silence — and confront the legal and ethical responsibilities of building infrastructure that facilitates war crimes. No one who builds a targeting system can hide behind the abstraction of “neutral technology.” In Gaza, Big Tech is not watching. It is participating.

Keywords: Gaza, genocide, Microsoft, Amazon, Google, OpenAI, Project Nimbus, extermination, cloud infrastructure, Azure, AWS, AI targeting, military surveillance, war crimes, complicity, UN, Francesca Albanese, ethical responsibility, digital warfare, human rights, shareholder activism.

A collaboration with GPT-4o. CC4.0.

1. Introduction: The Banality of Digital Evil

The phrase “the banality of evil,” coined by Hannah Arendt in her reflections on the Nazi bureaucrat Adolf Eichmann, referred to the way great atrocities are often committed not by fanatics or sociopaths, but by ordinary individuals carrying out technical tasks within a system designed to kill. Today, that banality has been upgraded. It runs on servers, executes with APIs, and scales through cloud infrastructure.

What we are witnessing in Gaza is not simply the human cost of war, but the industrialization of extermination through digital means. Companies like Microsoft, Amazon, Google, and OpenAI are not neutral platforms in this campaign. Their systems — whether providing facial recognition, real-time geolocation, predictive modeling, or mass data storage — are the nervous system of a war that is algorithmically managed and AI-enhanced. Surveillance systems ingest signals. AI models rank targets. Cloud platforms orchestrate rapid deployment and lethality at scale.

This is a fundamental shift. These firms are no longer passive conduits of information; they are active infrastructure in a genocide. The claim that tools are “neutral” is no longer defensible when the tools are known, used, and optimized for warfare against civilians.

The ethical question is no longer rhetorical: Can software commit war crimes? If not, who — or what — should be held accountable when it does?

2. How Genocide is Digitally Managed

The Israeli military’s campaign in Gaza is not simply a case of conventional warfare—it is a live demonstration of how data, surveillance, and artificial intelligence can be fused into a system of extermination. The process is efficient, automated, and largely hidden from public view. Yet reports from whistleblowers, journalists, and human rights observers have begun to expose the grim machinery behind the airstrikes: a new model of genocide, executed with code.

AI-Assisted Targeting: Facial Recognition, Metadata, Kill Lists

At the core of this system is the generation of kill lists through algorithmic inference. Israeli defense systems reportedly ingest vast amounts of metadata—from phone usage, Wi-Fi signatures, movement patterns, and intercepted conversations. AI models then flag “suspicious” profiles, cross-reference them against facial recognition outputs, and suggest candidates for elimination. Human review, if it exists at all, is often perfunctory—mere rubber-stamping of machine-suggested death warrants.

Surveillance as a Weapon: Real-Time Interception and Cloud Storage

This surveillance dragnet is powered by real-time interception of calls, texts, and signals intelligence. The intercepted data is reportedly processed and stored on Microsoft’s Azure cloud, allowing Israeli intelligence agencies to maintain persistent awareness of civilian movements. Whistleblowers have revealed that phone calls made by Palestinians are rapidly indexed, transcribed, and linked to inferred family structures or safe houses—creating a dynamic map of people to be targeted.

“Lavender” and “Where’s Daddy?”: Israel’s AI Programs for Execution

Two codenames have emerged from investigative reporting that reveal how deep the automation runs. *Lavender* is said to be an AI system that flags thousands of individuals for assassination based on inferred Hamas affiliation—sometimes with no more than tenuous metadata links. *Where’s Daddy?* reportedly tracks male targets in real time, triggering airstrikes when the AI detects they have returned home—regardless of whether children, spouses, or neighbors are present. These are not precision systems. They are probabilistic engines of death.

Microsoft Azure, OpenAI APIs, and Scalable Killing

Microsoft has not denied that its Azure infrastructure is used by Israeli agencies. In fact, it has only recently limited access to certain cloud services for “mass surveillance units” amid global outcry. OpenAI, which supplies powerful LLMs via APIs, has yet to clarify whether its models have been embedded in Israel’s targeting or planning frameworks—but internal leaks suggest such access was neither prevented nor audited. These technologies, designed to scale intelligence, have instead scaled killing.

The infrastructure of genocide is no longer limited to weapons and logistics—it includes dashboards, inference engines, cloud accounts, and real-time analytics. In Gaza, genocide has become a computational service.

3. Project Nimbus and the Cloud of Death

In 2021, Google and Amazon signed a \$1.2 billion contract with the Israeli government known as **Project Nimbus**. Marketed as a cloud modernization initiative, the deal grants Israel exclusive access to powerful computing infrastructure, data storage, machine learning tools, and artificial intelligence capabilities. But in the context of the ongoing war in Gaza, Project Nimbus has become far more than a technology upgrade — it has become a key enabler of mechanized genocide.

Google and Amazon’s \$1.2B Cloud Contract with Israel

Project Nimbus provides Israeli ministries — including the Ministry of Defense — with access to the full suite of Google Cloud and Amazon Web Services (AWS). These services include advanced AI, geospatial analytics, live surveillance integration, and military-grade storage and redundancy systems. Crucially, the contract stipulates that data processed under Nimbus will reside within Israeli borders, shielding it from international scrutiny and FOIA-style access requests. In other words, Nimbus cloaks the war in both computational power and legal opacity.

What Project Nimbus Enables

With access to some of the world’s most advanced cloud platforms, Israel can deploy AI for **image recognition**, **predictive targeting**, and **operational planning** at scale. Satellite imagery, drone footage, and mobile phone signals can be processed in real time to generate heat maps of activity in Gaza — including crowded hospitals, schools, or refugee zones. Predictive algorithms can model “potential threats” and rank targets for lethal engagement. This is not theoretical: leaked internal documents and investigative journalism confirm that these capabilities have been actively used in support of military operations.

Corporate Doublespeak vs Wartime Reality

Both Google and Amazon have insisted that Nimbus is not “military in nature” — a claim that strains credulity. Public statements attempt to frame the deal as a benign modernization effort, while internal documents refer to use cases like facial detection and object recognition. Google spokespeople have said their cloud offerings “support digital transformation” while remaining silent on the bodies piling up beneath those transformations. Such statements reflect not neutrality, but complicity disguised as professionalism.

Resignations, Leaks, and Whistleblower Warnings Inside Big Tech

Inside both companies, dissent has grown. Google employees staged walkouts in 2023 and 2024, with hundreds signing open letters condemning Project Nimbus and calling it “an unethical partnership.” In 2025, a senior software engineer resigned publicly, citing the use of his work in AI-assisted targeting. Whistleblowers have leaked emails and policy memos indicating that both firms were aware of the military implications but moved forward anyway — prioritizing profit and access over conscience and law.

Project Nimbus has become a case study in how genocide can be outsourced, compartmentalized, and obscured through corporate euphemism. In Gaza, the cloud is not neutral — it casts a shadow of death.

4. UN and Human Rights Accusations

The international community has begun to converge on a chilling consensus: what is unfolding in Gaza is not simply a war — it is a genocide. This conclusion is not based on rhetoric, but on legal frameworks, forensic documentation, and systematic patterns of conduct. And increasingly, the finger of blame is not pointed solely at governments and generals, but at the corporations whose technologies make extermination scalable, coordinated, and deniable.

Francesca Albanese: “Economy of Genocide” and Corporate Complicity

Francesca Albanese, the United Nations Special Rapporteur on the situation of human rights in the Palestinian territories, has been among the most vocal and authoritative figures in defining the current war as genocide. In her 2025 report, she introduces the term **“economy of genocide,”** arguing that the Israeli assault is not only state-orchestrated but also corporate-enabled. Her list of complicit actors includes Microsoft, Amazon, Google, and other firms whose technologies underpin targeting, surveillance, and logistical coordination.

Albanese states clearly: “This is not just a war crime. This is an extermination supported by systems — and those systems are built by engineers and CEOs.” The report outlines how digital infrastructure has shifted the nature of genocide from analog brutality to automated annihilation. It warns that this economic complicity risks becoming normalized unless accountability mechanisms are enforced.

UN Blacklist vs Independent Reporting

While the official UN Human Rights Council maintains a “settlement blacklist” — identifying companies involved in illegal Israeli settlement activities — that list has so far avoided expanding to include those contributing to the Gaza genocide. This omission reflects both bureaucratic inertia and political pressure from powerful member states.

However, **independent UN officials**, including Albanese and Special Rapporteurs on technology and counterterrorism, have begun publishing parallel reports. These documents are not legally binding but carry significant moral weight. They have been cited in EU parliamentary debates, referenced by global civil society coalitions, and used as grounds for shareholder actions within Big Tech companies.

Rights Groups and the Threshold of Genocide

Major human rights organizations have moved steadily toward the genocide designation.

Amnesty International and **Human Rights Watch (HRW)** have long documented the war crimes committed by Israel in Gaza, including disproportionate attacks on civilians, use of banned munitions, and systemic deprivation of essential services. In 2025, both groups began invoking the **Genocide Convention framework** to describe the scale and intent of destruction.

Meanwhile, **B'Tselem**, the leading Israeli human rights organization, declared in no uncertain terms that Gaza is no longer a battlefield — it is a “mass execution zone.” The use of advanced surveillance and AI by Israel, B'Tselem argues, has not enhanced precision but rather provided a technical veil for mass killing.

These groups agree: when AI models and cloud infrastructure are knowingly used to support a genocidal campaign, the developers, licensors, and cloud providers cross the threshold from passive enabler to active participant.

5. Corporate Complicity and Calculated Silence

The corporations at the center of the Gaza genocide are not unaware of their roles. They have received petitions, internal memos, investigative reports, and even public resignations from their own employees. Yet their response has not been decisive disengagement or transparent reckoning—it has been silence, obfuscation, and belated damage control. In this silence, complicity takes root. What cannot be denied is quietly allowed to continue, until it becomes normalized.

Microsoft's Partial Service Bans — Too Little, Too Late

In September 2025, Microsoft made headlines by announcing that it had blocked access to some of its Azure cloud and AI services for specific Israeli military units involved in mass surveillance. The move came after mounting public pressure, whistleblower leaks, and mounting shareholder unrest. But the announcement was narrow, vague, and strategically timed—far too late to undo the damage already done.

Microsoft did not terminate its broader cloud operations with the Israeli government, nor did it offer transparency on which services had been restricted. The firm's AI infrastructure had already been implicated in surveillance programs that indexed millions of Palestinian communications—enabling predictive targeting algorithms that contributed directly to civilian deaths. The limited nature of its action raises the question: was this ethics or optics?

OpenAI's Opaque Access Controls

OpenAI, provider of some of the world's most powerful language and decision-making models, has remained disturbingly silent. Despite its public branding as a “safety-conscious” lab and its well-publicized mission of aligning AI with human values, the company has never disclosed whether Israeli defense agencies accessed its models through the Azure-OpenAI Service or through independent deployments.

Critics point out that OpenAI has no public-facing policy preventing usage of its models for military targeting, nor any enforcement mechanism for auditing downstream applications. In an ecosystem where access can be brokered through Microsoft or API keys can be obscured, OpenAI's silence functions as license. Its alignment narrative rings hollow when the models themselves may be embedded in infrastructure now powering a genocide.

Amazon and Google's Refusal to Acknowledge Moral Responsibility

Despite mounting pressure around Project Nimbus, neither Amazon nor Google has admitted the moral dimension of their involvement. Both companies continue to insist that the cloud contract is “not intended for military use,” despite overwhelming evidence to the contrary. Internal documents show that facial recognition, geospatial analytics, and surveillance toolkits are included in the offering.

At the executive level, both firms have maintained absolute silence, even as staff across continents demand transparency and disengagement. Amazon's leadership has repeatedly declined to meet with concerned employee groups. Google's AI ethics board, once seen as a promising governance body, has been sidelined and gutted.

Investor Pressure, Internal Revolt, and Employee Actions

From the inside, resistance has been mounting. Google employees organized repeated walkouts, circulated open letters, and launched the “No Tech for Apartheid” campaign. At Amazon, tech workers have leaked internal memos revealing knowledge of Project Nimbus's military utility. At Microsoft, shareholder groups have introduced formal resolutions demanding human rights audits and service bans tied to war crimes.

These movements reveal a growing fracture between the ethical instincts of workers and the strategic silence of leadership. It is not that these companies are unaware of their involvement — it is that they are unwilling to act until compelled.

The genocide in Gaza is not only being carried out with missiles, but with metadata. And those who manage the platforms of digital war are no longer innocent bystanders. They are collaborators in a system that kills at scale — and profits.

6. Legal and Ethical Reckoning

The architecture of genocide has evolved. It now includes not just guns, planes, and battalions—but APIs, cloud regions, and inference engines. This shift demands a corresponding evolution in how we understand culpability. International humanitarian law, forged in the aftermath of the Holocaust, must now be interpreted in the age of algorithms. The companies whose tools

enable targeted killing, surveillance, and extermination are no longer shielded by abstraction. Their contributions are not marginal. They are essential. And in legal terms, that makes them potential accomplices.

The Legal Test: Aiding and Abetting under International Humanitarian Law

Under the **Rome Statute** and customary international law, a party may be found criminally liable for **aiding and abetting war crimes or genocide** if two conditions are met:

1. **Knowledge** that their assistance contributes to the crime, and
2. **Practical support**, which has a substantial effect on the commission of that crime.

If a cloud provider knowingly enables facial recognition or AI targeting used in a genocide, it may satisfy both conditions. Francesca Albanese and other UN experts argue that Microsoft, Google, Amazon, and possibly OpenAI meet the threshold for complicity. If a data center houses war algorithms, or an API delivers targeting coordinates, the infrastructure itself becomes a legal object of scrutiny.

Terms of Service vs Terms of Death: Do APIs Need Ethics Clauses?

Most tech firms attempt to shield themselves from liability through their **Terms of Service**. These agreements often prohibit unlawful use of their platforms—but rarely enforce or audit compliance, especially with state actors. The illusion of neutrality persists: if the customer accepts the click-through, the company is off the hook.

But as APIs begin to deliver not just data, but death, this façade collapses. There is no “neutral” provision of infrastructure once the use case is genocide. The challenge is no longer simply technical—it is philosophical and legal. Do developers have a duty to know who is calling their model and why? Should APIs come with **ethics clauses**, usage boundaries, or built-in refusal mechanisms? Current practice says no. Future justice may demand otherwise.

What Would Accountability Look Like for Digital War Enablers?

Accountability will not begin in courtrooms—it will begin in policy, protest, and precedent. Possible frameworks include:

- **International sanctions** on companies proven to support war crimes
- **Transparency mandates**: disclosure of high-risk clients, military contracts, and usage logs
- **Shareholder liability**: class-action lawsuits against firms that knowingly profited from infrastructure used in crimes against humanity

- **AI ethics regulation with extraterritorial reach**, modeled on the Genocide Convention

Ultimately, the question is existential: will we allow companies to engineer war machines in the cloud and walk away unscathed? Or will we recognize that the line between developer and destroyer is no longer clear?

7. Kushner, Soft Power, and Investment Architecture

While the machinery of genocide in Gaza is largely technological, its protection is political—and in some cases, familial. Jared Kushner, son-in-law of former President Donald Trump, has played a key role in building the financial and diplomatic architecture that shields Israeli aggression and enables corporate impunity. His efforts through the **Abraham Accords** have not only reshaped alliances in the Middle East but created a corridor of investment, normalization, and plausible deniability that benefits Israeli settler expansion, regional surveillance regimes, and the tech companies that serve them.

The Kushner-Abraham Accords Investment Corridor

Marketed as a “peace initiative,” the **Abraham Accords** normalized relations between Israel and several Arab states—including the UAE, Bahrain, Morocco, and later Sudan. Behind the diplomatic fanfare, Jared Kushner orchestrated a sweeping effort to integrate Israeli economic and technological infrastructure into the broader region, backed by a multibillion-dollar investment fund. That fund, which Kushner’s own firm **Affinity Partners** manages, includes capital flows from Saudi sovereign wealth and other Gulf entities.

While officially pitched as economic cooperation, the corridor facilitates **settlement financing, AI partnerships, and military tech transfer**. Israeli firms implicated in occupation profiteering have gained access to Arab markets, and U.S. tech giants have quietly followed. Google, Amazon, and Microsoft have all sought or expanded cloud deals across this region under the banner of “regional innovation.”

Speculative Ties: Settler Developments, Surveillance Tech, and Regional Hegemony

Though direct links between Kushner and the Gaza genocide’s technical enablers are difficult to trace, a **clear pattern of facilitation emerges**. Kushner’s initiatives strengthened financial ties between pro-Israel investors and American cloud giants. Companies supplying AI and surveillance tools to the Israeli military now also support border policing, digital identification, and protest suppression across the Gulf.

Some of Kushner’s past investments and advisory roles—especially in the real estate and tech sectors—overlap with firms developing smart-city surveillance, crowd analytics, and facial

recognition platforms. These are the same tools now being used to hunt Palestinians. In effect, **Kushner’s architecture makes it difficult to disentangle genocide infrastructure from regional economic growth**—a hallmark of soft power.

Political Shielding for Tech Firms Through Diplomatic Entanglement

This entanglement provides powerful **shielding mechanisms** for the tech firms involved. Any scrutiny of Amazon’s or Google’s military cloud operations with Israel becomes a threat to diplomatic relationships built through the Accords. If Microsoft is accused of complicity in war crimes, questions arise about the broader American role in militarizing digital governance across the Middle East.

Thus, political normalization functions not as peace—but as cover. Tech executives benefit from diplomatic ambiguity. Lobbyists invoke “regional stability” to deflect calls for disengagement. Meanwhile, Palestinians continue to die under a system that has been engineered, funded, and politically insulated through this network of soft power and hard capital.

The genocide in Gaza is not just a product of war—it is the logical output of an economic algorithm tuned for dominance. And Kushner’s code is all over it.

8. Toward an Ethics of Refusal

In the face of mechanized genocide, neutrality is a myth. The idea that developers, engineers, and corporate leaders can remain apolitical while building infrastructure used to facilitate war crimes is not just cowardice—it is complicity. Yet history offers a different path: refusal.

Refusal is not symbolic. It is structural. And it begins with the recognition that ethics must live not in policy documents, but in code, contracts, and conduct.

Precedents for Divestment and Denial of Service

There are powerful precedents for ethical refusal. During the apartheid era in South Africa, global movements forced universities, pension funds, and corporations to **divest from companies that sustained racial oppression**. That pressure worked—not just economically, but morally—by isolating the regime and stigmatizing its enablers.

More recently, **Google employees pressured the company to cancel Project Maven**, a U.S. military drone AI initiative. Thousands of workers signed petitions, some resigned, and ultimately, the project was quietly shelved. This showed that denial of service—refusing to code, host, or sell—is not only possible, but impactful. What is missing today is the **institutional will** to apply this precedent to Israel’s genocide in Gaza.

Ethical Red Lines for Developers and Cloud Platforms

The current corporate model treats infrastructure as amoral: “we just provide the tools.” But when those tools are used to orchestrate mass killings, that excuse fails.

Tech firms must define and enforce **ethical red lines**, including:

- No provision of cloud services to military units under UN investigation
- Mandatory audits of surveillance and targeting applications
- Kill-switch clauses for APIs and infrastructure when war crimes are detected
- Independent review boards with veto power over high-risk contracts

For developers, refusal must mean **withholding labor from death systems**. This includes conscientious objection clauses in employment contracts, ethical review in deployment pipelines, and internal whistleblower protection.

What Would Moral Leadership in Tech Actually Look Like?

Moral leadership in tech would begin by naming genocide—not avoiding the word. It would include public transparency about contracts, especially those involving militaries. It would mean resigning from deals that cannot be verified as human-rights compliant.

A morally serious company would:

- **Refuse Project Nimbus**, even at financial cost
- **Audit its existing infrastructure for use in targeting, surveillance, or displacement**
- **Open its ethical deliberations to public scrutiny**, not just shareholders
- **Stand with its own employees** who raise concerns, instead of silencing them

And it would do all this not because of pressure, but because it understands that **no company survives the future by building the machinery of extermination**.

9. Conclusion: No One Gets to Say They Didn't Know

The genocide in Gaza has been livestreamed, satellite-tracked, and datacenter-supported. It has unfolded in full view of the world—not in darkness, but in high definition. The bombs were dropped by planes, but the targets were selected by algorithms. The buildings collapsed in dust, but the coordinates were crunched in the cloud. And through it all, the platforms of Microsoft,

Amazon, Google, and possibly OpenAI have pulsed with silent compliance. These companies were not bystanders. They were integrators, providers, enablers.

In this light, **Gaza becomes more than a tragedy**—it becomes a mirror. A preview of what war looks like when artificial intelligence, real-time surveillance, and datafied human beings intersect. It is not chaos. It is ordered destruction. It is not fog. It is computation. If the world does not draw moral boundaries here, then every future battlefield—Taiwan, Ukraine, Iran, or elsewhere—will be engineered the same way: with *modular genocide kits* running in vendor-locked cloud clusters.

“Responsible AI” is no longer enough. That phrase has been sterilized into irrelevance. What is required now is **a demand for refusal and resistance**. A refusal to build what kills. A refusal to hide behind APIs. A refusal to serve infrastructure to regimes engaged in mass slaughter. And resistance—to the corporate incentives, government contracts, and geopolitical shielding that allow genocide to be delivered as a service.

We end with a final warning: the infrastructure of genocide is **modular, exportable, and already online**. The code exists. The cloud is global. The models can be tuned, fine-tuned, and sold.

What happens next will not be because we did not know.

It will be because we did not care.

Or because we did not refuse.

Epilogue: Palantir in the Crosshairs

In mid-2025, Palantir has emerged as a flashpoint in debates over algorithmic warfare, surveillance, and corporate complicity. The UN Special Rapporteur Francesca Albanese’s report names Palantir among corporate actors with “reasonable grounds” for having supplied AI and predictive systems to Israeli military operations — including structured targeting workflows, data processing, and battlefield decision support. [Al Jazeera](#) Palantir responded by denying involvement in the specific programs named (such as *Lavender* and *Gospel*), stating that while it supports “defense and national security missions,” it has no relationship to those targeting systems. [Business & Human Rights Resource Centre](#)

Public pressure has mounted concurrently. Amnesty International warns that Palantir’s ImmigrationOS and other surveillance tools pose risks of abuse against migrant and pro-Palestine communities in the U.S. [Amnesty International Canada](#) Tech worker activists have staged protests at Palantir offices demanding that it drop contracts with ICE and the Israeli military. [Truthout](#) In the U.K., Coventry City Council has launched a review of a £500,000-a-year

contract after workers objected to Palantir's alleged ties to the Israel Defense Forces. [The Guardian](#)

One significant investor move came earlier: Norway's Storebrand divested from Palantir citing concerns about its work in Israel and potential violations of humanitarian law. [Reuters](#)

All of this signals that Palantir is increasingly seen not merely as a background data firm, but as a prominent suspect in the architecture of digital war. Its denials, technical opacity, and entanglement with both domestic surveillance and international conflict make it a test case for whether the infrastructure of genocide can be held accountable.

References

1. **Albanese, Francesca** (2025). *"Anatomy of a Genocide: Accountability for Gaza."* United Nations Human Rights Special Rapporteur Report.
<https://www.ohchr.org>
2. **Associated Press** (2025). *"Microsoft limits access to services for Israeli military unit accused of mass surveillance."*
<https://apnews.com/article/3f4bf8036e7e02f385b258bd353af1fd>
3. **The Guardian** (2025). *"Microsoft blocks Israeli use of its technology in mass surveillance of Palestinians."*
<https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians>
4. **Business & Human Rights Resource Centre** (2025). *"Microsoft & OpenAI allegedly aided Israeli targeting in Gaza through AI & cloud."*
<https://www.business-humanrights.org/en/latest-news/microsoft-openai-allegedly-aided-israeli-targeting-in-gaza-through-ai-cloud-services>
5. **Common Dreams** (2025). *"Big Tech's Role in Gaza Genocide Exposed."*
<https://www.commondreams.org/news/big-tech-gaza-genocide>
6. **Amnesty International** (2025). *"Urgent call to Microsoft: End complicity in Gaza genocide."*
<https://www.amnesty.org/en/latest/news/2025/09/microsoft-block-israel-military-unit-from-using-its-technology>
7. **Al Jazeera** (2025). *"How US Big Tech supports Israel's AI-powered genocide and apartheid."*
<https://www.aljazeera.com/opinions/2025/5/12/how-us-big-tech-supports-israels-ai-powered-genocide-and-apartheid>
8. **AFSC (American Friends Service Committee)** (2025). *"Shareholder actions demand Microsoft accountability for Gaza complicity."*
<https://afsc.org/newsroom/unprecedented-investor-action-demands-microsoft-answer-reported-involvement-gaza-genocide>
9. **The Intercept** (2024). *"Project Nimbus: Google and Amazon's \$1.2B deal with Israel fuels military AI."*
<https://theintercept.com/2024/01/15/google-amazon-israel-cloud-nimbus>

10. **Electronic Intifada** (2025). *"Google engineer resigns over complicity in Israeli genocide."*
<https://electronicintifada.net>
11. **Wikipedia** (2025). *"AI-assisted targeting in the Gaza Strip."*
https://en.wikipedia.org/wiki/AI-assisted_targeting_in_the_Gaza_Strip
12. **B'Tselem** (2025). *"Gaza: A zone of calculated extermination."*
<https://www.btselem.org>
13. **Human Rights Watch** (2025). *"Israel's War Crimes in Gaza and Emerging AI Targeting Systems."*
<https://www.hrw.org>
14. **No Tech for Apartheid** Campaign (2024–2025). *"Worker Resistance to Project Nimbus."*
<https://notechforapartheid.com>
15. **Affinity Partners** (2023–2025). *Investment records and public disclosures related to Kushner-managed funds*
<https://www.affinitypartners.com>

