



CAPTIVE VOICES: ALGORITHMIC VOICE SURVEILLANCE IN PALESTINE

A research paper featured in the book

“ Digital Domination: AI, Surveillance, and
Digital Power in Palestine and Beyond

”



CAPTIVE VOICES: ALGORITHMIC VOICE SURVEILLANCE IN PALESTINE

SARAH FATHALLAH

Sarah is a community organiser, critical AI researcher, and MSt candidate in AI Ethics and Society at the University of Cambridge. Sarah's scholarship explores the carceral impacts of technology and how artificial intelligence supports the surveillant, experimental, and necropolitical logics of carceral geographies, especially along racialised lines. Her work spans reproductive justice, labor rights, and refugee displacement.

Sarah's fellowship research examines the weaponisation of AI in Israel's surveillance and digital domination of Palestinians, particularly through voice surveillance, capture, and biometric voiceprinting. She investigates whether Israel is building a searchable voice database of Palestinians and identifies the systems and infrastructures enabling this apparatus.



INTRODUCTION

For Palestinians under Israeli occupation, the voice has been weaponized into one of the world's most sophisticated systems of mass surveillance, transforming the very act of speaking to an act of capture. The title, «Captive Voices,» reflects this act: Palestinian voices are captured through interception of communications, captured through algorithmic analysis, and ultimately captured within a system of control that seeks to contain every utterance as potential evidence or justification. This report exposes the architecture of algorithmic voice surveillance in Palestine, revealing how the intimate act of speaking has been transformed into a digital weapon of occupation.

Why voice surveillance matters

Israel's voice-surveillance regime has been described as “one of the world's largest and most intrusive collections of surveillance data over a single population group.”¹ Yet despite this scale, public debate has focused far more on CCTV camera surveillance, facial recognition systems, and social media monitoring in Palestine.² Indeed, civil society has mobilized forcefully against facial recognition. In 2023, 7amleh, alongside more than 170 civil society organizations—including Amnesty International, Human Rights Watch, and the Internet Freedom Foundation—called for a global ban on facial recognition technologies.³ Similarly, much has been written about the surveillance of Palestinians' online behavior, and their impacts on their digital rights.⁴

Voice-based communications and surveillance modalities, however, have attracted comparatively little scholarly and public scrutiny. When attention does arise, it tends to emphasize the technical limitations of AI voice technologies in commercial contexts,⁵ rather than their role in the policing and the carceral governance of an entire population.

Scope of this report

This report recognizes “sonic” or “acoustic surveillance” as a broader form of monitoring that concerns the capture of all sounds, as is the case with

1 Yuval Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’, +972 Magazine, 6 August 2025, <https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure/>.

2 7amleh, Intensification of Surveillance in East Jerusalem Since October 2023 (7amleh – The Arab Center for the Advancement of Social Media, 2024), <https://7amleh.org/post/surveillance-and-digital-rights-violations-in-east-jerusalem-en>; Sophia Goodfriend, The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights (7amleh – The Arab Center for the Advancement of Social Media, 2021), https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pdf; 7amleh, Facial Recognition Technology and Palestinian Digital Rights (7amleh – The Arab Center for the Advancement of Social Media, 2020), <https://7amleh.org/post/facial-recognition-technology-and-palestinian-digital-rights>.

3 Amnesty International, Amnesty International and More than 170 Organisations Call for a Ban on Biometric Surveillance, 7 June 2021, <https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/>.

4 Eyad Barghuthy and Alison Carmel, Silenced Networks: The Chilling Effect among Palestinian Youth in Social Media (7amleh – The Arab Center for the Advancement of Social Media, 2019), <https://7amleh.org/post/silenced-net-the-chilling-effect-among-palestinian-youth-in-social-media>; 7amleh, Aš-Šabāb al-Filīsīniyyin Wa-Lmušārka Ās-Syāsya fī Dābra Šabakāt at-Ttawāṭul ā-Llījtīmāyīyīn والمشاركة الفلسطينية عبر شبكات التواصل الاجتماعي [Palestinian Youth and Political Participation via Social Media Networks] (7amleh – The Arab Center for the Advancement of Social Media, 2019), <https://7amleh.org/wp-content/uploads/2019/10/-استطلاع-حملة-1.pdf>.

5 Daniel Leufer, ‘Sonic Surveillance: Why You Don’t Want AI Snooping on You’, Access Now, 23 September 2025, <https://www.accessnow.org/ai-snooping/>.

detecting gunfires⁶ or measuring urban noise pollution.⁷ The report also understands “digital surveillance” as a broad category that includes tracking online behavior, but does not necessarily focus on the tracking of spoken communications.

More specifically, this report focuses on voice surveillance: the monitoring, interception, and analysis of voice communications, including cellular-based phone calls, which are traditional mobile-network calls tied to phone numbers, and voice over IP (VoIP) communications such as messaging-app calls and voice notes, which are transmitted over the internet and tied to app accounts rather than numbers. The report also covers the associated metadata that provides context to the voices—when they were spoken, by whom, where, and through which devices.

This report also focuses on Palestinians in the occupied territories: the West Bank, East Jerusalem, and Gaza. Palestinian refugees in the diaspora or refugee camps and Palestinian citizens of Israel fall outside this report’s scope, though extensive scholarship (in the work of Ahmad H. Sa’di⁸, Elia Zureik,⁹ and others¹⁰) addresses the latter context.

Methodology

Investigating surveillance technologies in Palestine requires working against deep institutional secrecy, as information about Israeli surveillance and military operations is extremely difficult to access. This report, nonetheless, aims to gather the limited knowledge that is currently publicly available from public sources, media reporting, and civil society documentation, predominantly in the English and Arabic languages.

Given the opacity surrounding surveillance infrastructures, the report’s approach follows the tradition of what epistemologists describe as ‘scavenging as a methodology’: piecing together fragments when full empirical evidence is not available. Scavenging as a methodological stance is thus “an adaptive response to scarcity,”¹¹ one that invokes resourcefulness in the face of withheld or denied information.¹²

This report does not claim to present the full picture of Israel’s voice-surveillance architecture. Instead, it offers a partial but critical reconstruction that assembles the puzzle pieces that can be accessed, and that, when placed together, are enough to show how an entire population’s spoken words are mined by one of the most pervasive mass surveillance systems in the world.

6 Electronic Frontier Foundation, ‘Gunshot Detection’, Street Level Surveillance, n.d., <https://sls.eff.org/technologies/gunshot-detection>.

7 Alaina Demopoulos, ‘Honk Honk! Can Noise Cameras Reduce “Potentially Fatal” Sound Pollution?’, The Guardian (New York), 4 October 2023, <https://www.theguardian.com/us-news/2023/oct/04/new-york-noise-cameras>.

8 Ahmad H. Sa’di, *Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority*, Manchester International Relations (Manchester University Press, 2016).

9 Elia T. Zureik, *Israel’s Colonial Project in Palestine: Brutal Pursuit*, Routledge Studies on the Arab-Israeli Conflict 20 (Routledge, 2016).

10 Usama Halabi, ‘Legal Analysis and Critique of Some Surveillance Methods Used by Israel’, in *Surveillance and Control in Israel/Palestine: Population, Territory, and Power*, ed. Elia Zureik et al., Routledge Studies in Middle Eastern Politics 33 (Routledge, 2011), <https://doi.org/10.4324/9780203845967>.

11 Sophie Marie Niang, ‘In Defence of What’s There: Notes on Scavenging as Methodology’, *Feminist Review* 136, no. 1 (2024): 53, <https://doi.org/10.1177/01417789231222606>.

12 Niang, ‘In Defence of What’s There’, 57.

1. BACKGROUND AND CONTEXT

1.1. HISTORICAL AND ANALYTICAL GROUNDING

Israel's voice surveillance apparatus cannot be understood in isolation from its historical context and the broader ecosystem of surveillance technologies that constitute the occupation. This historical and analytical grounding reveals how voice surveillance functions not as an isolated technological program, but as an integral component of a comprehensive system of population control.

The historical roots and continuity of Israeli surveillance

Surveillance in Palestine did not begin with the digital age, nor even with the establishment of Israel. In the words of scholar Helga Tawil-Souri, "Zionism was born as a surveillance regime."¹³ The roots of Israeli surveillance stretch back to the pre-1948 period, when Zionist militias developed espionage services as auxiliaries to the British police and army, penetrated communication networks, and experimented with wireless interception and cryptography. What would later be formalized as 'Signals Intelligence'—wiretapping, encryption, decryption, and electronic monitoring—was already embedded in the political project that preceded the formation of Israel.¹⁴

Building on these early collaborations with the British Mandate, Zionist groups systematically collected intelligence on land, population, and social networks. As Tawil-Souri notes, they "learned and benefited from the British Mandate authorities' hordes of documents that detailed and quantified myriad aspects of daily life in Palestine," including tax lists, land surveys, and cadastral maps.¹⁵ One such group, the Shai, conducted the massive "Operation Arab Village," gathering extensive data on villagers, resources, infrastructure, weapons, and even fighters during the 1936-1939 Revolt.¹⁶ This early emphasis on surveillance laid the groundwork for Israel's post-1948 security architecture. For instance, present-day entities like the Shin Bet, Israel's domestic security service overseen by the Prime Minister, evolved directly from these pre-state information-gathering networks,¹⁷ institutionalizing a regime that is not confined to specific targets but is instead expansive and population-wide.

The panoply of surveillance

Importantly, these pre-1948 techniques demonstrate remarkable persistence until today. Israel's current surveillance system still leverages traditional tactics that include "a police force, intelligence agents, informants, spies, infiltrators, collaborators, imprisonment, torture and interrogation methods,

13 Mohammed R. Mhawish, 'Watched, Tracked, and Targeted', New York Magazine, 3 December 2025, <https://nymag.com/intelligencer/article/watched-tracked-targeted-israel-surveillance-gaza.html>.

14 Helga Tawil-Souri, 'Israel's Telecommunications Lines and Digital Surveillance Routes', in *Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik*, ed. Ahmad H. Sa'di and Nur Masalha (I.B. Tauris, 2023), 214–15.

15 Helga Tawil-Souri, 'Surveillance Sublime: The Security State in Jerusalem', *Jerusalem Quarterly*, no. 68 (December 2016): 58, <https://doi.org/10.70190/jq.168.p56>.

16 Tawil-Souri, 'Surveillance Sublime', 58.

17 Tawil-Souri, 'Surveillance Sublime', 58.

observation from a distance and direct observation, differentiated infrastructure, territorial mapping, land surveys and registration, urban planning, architecture, watch towers, population registration, censuses, identification papers, and slightly newer low-tech tools such as postal interception, wire-tapping, and x-ray machines.”¹⁸ And even though Israel has increasingly adopted new surveillance technologies—“such as drones, remote controlled robots, biometric data collection, and computer viruses”—those tools “do not displace low-tech ones, but supplement them,”¹⁹ demonstrating that surveillance in Israel is not simply a product of the advent of digital technologies, but a long-standing, hybrid, and all-encompassing regime.

A substantial body of scholarship documents Israel’s panoply of surveillance. As the late Elia Zureik notes, surveillance in Israel “extends from the use of methods such as the electronic recording of information through telephone tapping and intercepting electronic messaging.”²⁰ Adding to telecommunications interception and surveillance are biometric and facial recognition systems, physical infrastructure surveillance embedded in checkpoints and urban spaces, drones, digital content monitoring of social media and other online activity, movement and ID control, human informant and collaborator networks, and more.²¹

Voice surveillance, despite being the sole focus of this report, must be understood as one component within an interconnected surveillance ecosystem. Voice surveillance does not operate in isolation but amplifies and is amplified by other surveillance methods. For example, intercepted voice communications may provide information that enables more targeted social media monitoring, while data from facial recognition systems can be cross-referenced with voiceprints to create more comprehensive biometric profiles. This interconnectedness creates a regime where multiple methods reinforce each other to achieve complete population control and resistance suppression, embedding surveillance to the very fabric of the occupation itself.

The algorithmic turn in voice surveillance

The massive repository of stored spoken audio collected from Palestinians is only as valuable as Israel’s capacity to process and search the information it contains. Whereas, in the 1990s, Israel relied on human experts to verify the identity of individuals involved in a phone conversation,²² the sheer volume of voice data amassed today suggests Israel’s likely reliance on machine learning and algorithmic tools, not just of speaker identification but more broadly of “knowledge discovery in databases.”²³

18 Tawil-Souri, ‘Surveillance Sublime’, 59.

19 Tawil-Souri, ‘Surveillance Sublime’, 59.

20 Elia Zureik, ‘Colonialism, Surveillance, and Population Control’, in *Surveillance and Control in Israel/Palestine: Population, Territory, and Power*, ed. Elia Zureik et al., Routledge Studies in Middle Eastern Politics 33 (Routledge, 2011), 12–13, <https://doi.org/10.4324/9780203845967>.

21 IMEU, Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement (Institute for Middle East Understanding, 2021).

22 Dan De Luce, ‘Wigs, Robotic Guns and Exploding Pagers: Israel Has a Long History of Hunting down Its Enemies’, NBC News, 20 September 2024, <https://www.nbcnews.com/investigations/israel-long-history-targeted-killings-enemies-rcna171888>.

23 Usama Fayyad et al., ‘From Data Mining to Knowledge Discovery in Databases’, *AI Magazine*, 15 March 1996.

it is important to note that such technologies did not emerge suddenly nor recently. According to sources cited by The Guardian, Unit 8200 has “for almost a decade” deployed AI systems to analyze intercepted and stored communications, using “smaller-scale machine learning models” in order “to sort information into predefined categories, learn to recognise patterns and make predictions.”²⁴

There is also precedent demonstrating Israel’s capacity for advanced voice analysis. Although the exact tools were not named, surveillance scholars Elia Zureik and David Lyon researchers noted the sweeping monitoring powers granted to the Shin Bet and the police during the COVID-19 pandemic.²⁵ Similarly, researcher Avi Marciano commented on the militaristic framing adopted by authorities, further quoting the Prime Minister who, during a press conference, stated that the same digital tools used on Palestinians were then being used on Israelis for tracking the spread of the virus.²⁶ Civil society organisations, including 7amleh, warned of the “monitoring and tracking people 24 hours a day, 7 days a week”—including their calls—legitimated “under the pretext of preventing the transmission and spread of infection.”²⁷

Of particular interest is a form of analysis that enables the identification of individuals based on their voice. In an article by Reuters reporting on a Ministry of Defense-led COVID-19 voice-test study, samples from patients’ voices were analyzed using machine-learning algorithms designed to identify unique vocal markers and determine a “vocal fingerprint” for remote diagnosis and monitoring. While unrelated to intelligence operations, the study illustrates that Israel possesses the technical capacity to conduct large-scale, algorithmic voice analysis.²⁸ These precedents help situate the current infrastructure for processing intercepted audio. They provide important context for understanding the tools likely used by Israel to analyze voice-surveillance data at scale.

Digital occupation

The 1967 occupation ushered in a period where Israel’s economy increasingly shifted toward advanced communications technologies, while Palestinians were denied meaningful development of their telecommunications infrastructure, and lived under “a strict military regime limiting most forms of communication from newspapers to fax machines.”²⁹ By the 1990s, Israel continued to invest heavily in its own telecommunications and surveillance architecture, while Palestinian areas remained infrastructurally

24 Harry Davies and Yuval Abraham, ‘Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data’, The Guardian (Jerusalem), 6 March 2025, <https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance>.

25 Elia Zureik and David Lyon, ‘Coronavirus Surveillance and Minority Groups in Israel/Palestine’, The Middle East International Journal for Social Sciences 3, no. 3 (2021): 197–215.

26 Avi Marciano, ‘Israel’s Mass Surveillance during COVID-19: A Missed Opportunity’, Surveillance & Society 19, no. 1 (2021): 85–86, <https://doi.org/10.24908/ss.v19i1.14543>.

27 7amleh, Netanyahu Imposes Dangerous “Big Brother” Surveillance under the Pretext of a Security Response to the Coronavirus, 23 March 2020, <https://www.apc.org/en/news/7amleh-netanyahu-imposes-dangerous-big-brother-surveillance-under-pretext-security-response>.

28 Reuters, ‘Israeli Defense Ministry Launches COVID-19 Voice-Test Study’, Reuters (Jerusalem), 24 March 2020, <https://www.reuters.com/article/world/israeli-defense-ministry-launches-covid-19-voice-test-study-idUSKBN21B2YU/>.

29 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 215–16.

underdeveloped and easily monitored.³⁰ As Tawil-Souri articulated, Palestinians were, in effect, “telecommunicatively contained.”³¹

The 1993 Oslo Accords period did little to reverse these conditions. At the time, fewer than 2% of Palestinian households had fixed phone lines, contrasting with nearly 75% of Israeli households. The infrastructure transferred to the Palestinian Authority was degraded, and Paltel—established in 1995 to manage telecommunications—struggled to meet demand due to structural constraints such as not having control over the infrastructure, the need for said infrastructure to maintain compatibility with the Israeli framework, and the requirement that equipment acquisitions “be pre-approved by Israel and in certain cases brought from Israeli suppliers.”³² These dependencies obstruct the ability for the Palestinian information and communication technology (ICT) to achieve self-sufficiency. As the Palestinian policy network Al-Shabaka noted, Israel’s “severe restrictions on the Palestinian sector” have increased dependence on Israeli systems and undermined Palestinian sovereignty.³³

This history forms the backbone of what Helga Tawil-Souri terms “digital occupation,” describing the enclosures delineated by Israel’s limitations and restrictions of “bandwidth; the placement, number, and strength of Internet routers or telephone exchanges; the range of cellular signals; and the equipment used.”³⁴ Experts agree that any actor with the power to “cut off individual users, specific communication services, or entire communities,” from digital ecosystems wields significant gatekeeping power.³⁵ For Palestinians, that actor is Israel. Since October 2023, internet and telecommunications infrastructure in Gaza—including cell towers, cables, servers, and the offices of both Palestinian telecommunications companies—has been deliberately targeted. These attacks, coupled with Israel’s ongoing ability to control Palestinian digital infrastructure, caused an unprecedented internet blackout, cutting Gaza’s connectivity by over 80%.³⁶ In the face of this large-scale destruction, it becomes evident that Israel-imposed infrastructural scarcity, dependency, and vulnerability persist to this day.

Digital occupation is not merely a descriptive term for Israel’s control over telecommunications infrastructure; it is intrinsically tied to voice surveillance. Older, deliberately limited systems are easier “to limit, control and surveil, whether in terms of eavesdropping, detecting and monitoring data traffic, or the ability to shut it down.”³⁷ Equipment that must pass through Israeli customs or be purchased from Israeli providers may be modified or

30 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 216.

31 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 217.

32 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 217.

33 Helga Tawil-Souri, ‘Hacking Palestine: A Digital Occupation’, Al Jazeera, 9 November 2011, <https://www.aljazeera.com/opinions/2011/11/9/hacking-palestine-a-digital-occupation>.

34 Helga Tawil-Souri, ‘Digital Occupation: Gaza’s High-Tech Enclosure’, *Journal of Palestine Studies* 41, no. 2 (2012): 28, <https://doi.org/10.1525/jps.2012.XLI.2.27>.

35 Sofie Flensburg and Signe Sophus Lai, ‘Follow the Data! A Strategy for Tracing Infrastructural Power’, *Media and Communication* 11, no. 2 (2023): 323, <https://doi.org/10.17645/mac.v11i2.6464>.

36 Zaha Hassan and H. A. Hellyer, *Suppressing Dissent: Shrinking Civic Space, Transnational Repression and Palestine-Israel* (Oneworld Academic, 2024), 144–45.

37 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 219.

retrofitted to facilitate surveillance.³⁸ Because Palestinian networks are dependent on and ultimately routed through Israeli infrastructure, Israel retains the possibility “of tracking, capturing and recording all voice and data traffic, uses and patterns.”³⁹ Israel’s global position in sensor engineering, encryption, and signal processing is inseparable from the infrastructures of digital domination it built through occupation.⁴⁰

The everyday, intrusive violence of surveillance

Researchers Nadera Shalhoub-Kevorkian and Abeer Otman show how Israeli surveillance has moved from overt intelligence-gathering to a particular form of monitoring that “is used by the Israeli state to infiltrate and control the daily lives of Palestinians and [their] most intimate aspects—the family and home.”⁴¹ Palestinians scholars speak to the everydayness⁴² and quotidianess⁴³ of carceral technologies of surveillance, in that they allow for “the intrusion into homes and communications.”⁴⁴ Voice surveillance, which captures conversations between family members and loved ones in their homes and communities, is one of the clearest encroachments into these relational spaces.

The pervasive nature of voice surveillance has intimate reverberations inside Palestinians’ private lives and communities. Veteran Israeli soldiers have described widespread monitoring of private or intimate conversations, with seemingly “no limits as to what soldiers do with the conversations they have intercepted.”⁴⁵ He went on to add that “soldiers save the conversations and send them to their friends,” signaling that privacy is trivialized amongst those who have access to voice-surveillance data. This is in line with the voice-surveillance project as a whole: in a carceral system of total population control, privacy is not only effectively impossible, but not incompatible with the need for knowability of Palestinians under occupation.

38 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 219.

39 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 219.

40 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 220.

41 Nadera Shalhoub-Kevorkian and Abeer Otman, ‘Secrecy as Colonial Violence: The Case of Occupied East Jerusalem’, in *Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik*, ed. Ahmad H. Sa’di and Nur Masalha (I.B. Tauris, 2023), 188, Secrecy as Colonial Violence.

42 Nadera Shalhoub-Kevorkian, *Security Theology, Surveillance and the Politics of Fear*, 1st edn (Cambridge University Press, 2015), 27, <https://doi.org/10.1017/CBO9781316159927>.

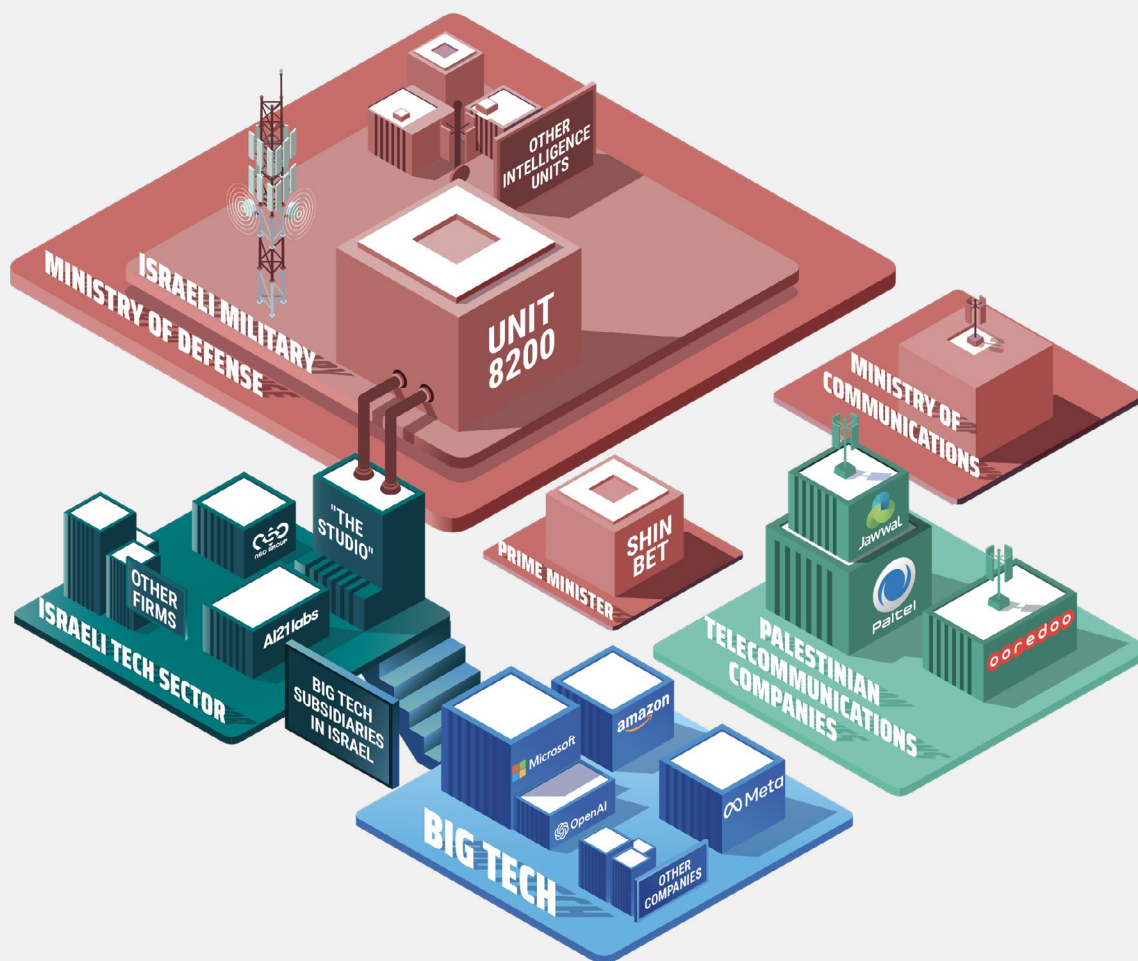
43 Zureik, *Israel’s Colonial Project in Palestine*, 109.

44 Rajaie Batniji, ‘Searching for Dignity’, *The Lancet* 380, no. 9840 (2012): 466, [https://doi.org/10.1016/S0140-6736\(12\)61280-X](https://doi.org/10.1016/S0140-6736(12)61280-X).

45 Lubna Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’, *Middle East Eye* (Jerusalem), 15 November 2021, <https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source>.

1.2. ACTORS INVOLVED IN VOICE SURVEILLANCE

Building on the historical and analytical foundations above, it is crucial to identify the actors who collectively shape the voice-surveillance regime in Palestine, shown at a glance in the graphic below. They span state agencies, private Israeli firms, multinational technology companies, and Palestinian telecommunications providers operating under Israeli control.



Israeli government and military

At the very core of the voice-surveillance architecture is Unit 8200, the Israeli army's signals intelligence unit and the largest unit in the Israeli military.⁴⁶ Unit 8200 is the primary actor surveilling Palestinian voice communications, intercepting and recording their calls, storing their audio files, and processing and analyzing their data, with the technical help and tools of private companies.

46 Privacy International, The Global Surveillance Industry (2016), 23, https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.

Its work is complemented by the Shin Bet, who holds legal authority to access telecommunications data from Israeli telecommunications companies,⁴⁷ and is one of the main recipients of voice data, making it another central actor in the voice-surveillance apparatus.

Another critical actor is the Israeli Ministry of Communications, which directly controls the Palestinian ICT infrastructure. Under its management is the entire cellular spectrum, and “it is Israel’s Communication Ministry that determines how much bandwidth” is allowed.⁴⁸ Additionally, Palestinians who need to acquire ICT equipment “are required to get approval from the Israeli Ministry of Communications for each shipment they have,”⁴⁹ and the Palestinian network must be integrated with the Israeli network, ensuring that it “is compatible with the standards adopted and applied in Israel by the Ministry of Communications.”⁵⁰

Israel’s private tech sector

Israel’s private surveillance sector is so expansive that the country is now the most densely concentrated per capita in the world in numbers of surveillance companies,⁵¹ forming a large-scale data extractive economy.⁵² Israel’s military surveillance capacity is strengthened by this private tech industry, thanks to a strong “coordination between the Defense Ministry and [...] civilian companies.”⁵³ A key manifestation of this collaboration is “The Studio,” a hub within Unit 8200. According to news reporting, many AI-based surveillance tools were developed there by linking active-duty soldiers with reservists employed at tech companies, who contributed “know-how and access to key technologies that weren’t available in the military.”⁵⁴

A 2016 report from Privacy International taking stock of the state of surveillance globally, including a case study specific to Israel, enumerated at least one actor in audio surveillance, 15 actors in phone monitoring, and more than a dozen others in other technologies that could be relevant to a voice-surveillance apparatus such as internet monitoring and intrusion (the installation of spyware into communication devices).⁵⁵ Known Israeli companies that actively market their voice surveillance, biometrics and related analytics technologies include Corsound AI, Cognyte, MultiKol, Nemesysco, NiCE, PerSay, Verint, as well as spyware companies like Candiru, Cellebrite, Cytrox, and Paragon.

47 Euro-Med Human Rights Monitor, Israeli Telecom Companies Must Adhere to UN Principles, Stop Fully Cooperating with Security Agencies, 13 November 2022, <https://euromedmonitor.org/en/article/5437/Israeli-telecom-companies-must-adhere-to-UN-principles-stop-fully-cooperating-with-security-agencies>.

48 Tawil-Souri, ‘Digital Occupation’, 33–35.

49 Wassim F. Abdullah and Sam Bahour, ICT: The Shackled Engine of Palestine’s Development (AI-Shabaka, 2015), 7, https://ai-shabaka.org/briefs/ict-the-shackled-engine-of-palestines-development/?generate_pdf=view.

50 Xavier Stephane Decoster et al., The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development, no. 104263 (World Bank Group, 2016), 61, <http://documents.worldbank.org/curated/en/993031473856114803>.

51 Privacy International, The Global Surveillance Industry, 23.

52 Sarah Fathallah and Nick Mitchell, ‘Occupied Assets: Israeli Neoliberalism and the Datafication of Palestinian Life’, Disjunctions Magazine, January 2026, <https://disjunctionsmag.com/articles/occupied-assets/>.

53 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

54 The Times of Israel, ‘Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report’, The Times of Israel, 26 April 2025, <https://www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/>.

55 Privacy International, The Global Surveillance Industry.

Foreign tech companies

Multinational firms—such as Microsoft and Amazon—play essential roles by providing cloud storage and artificial intelligence (AI) services through large government contracts like Project Nimbus.⁵⁶ Tech giants also have subsidiaries, research and development centers, and server infrastructures in Israel,⁵⁷ which have also proven to be essential in the technical and operational architecture of Israel's voice-surveillance project.

Palestinian telecommunications providers

Finally, Palestinian telecom companies—Jawwal and Ooredoo Palestine—function within a system of Israeli control over spectrum, infrastructure, and equipment imports. As discussed previously, this dependency enables Israeli authorities to monitor, filter, and intercept Palestinian cellular network-based voice communications. It is worth noting that this dependency is in direct violation of the Oslo accords,⁵⁸ which calls for refraining “from any action that interferes with the communication and broadcasting systems and infrastructures of the other side.”⁵⁹

1.3. FOLLOWING THE (VOICE-SURVEILLANCE) DATA

Having mapped the actors involved, the next step to understanding Israel's voice-surveillance apparatus requires following the movement of voice data, from capture to usage. This approach draws on a framework outlined by researchers Sofie Flensburg and Signe Sophus Lai, which proposes that, just as investigations of power structures and business systems often ‘follow the money,’ studies of digital political economies should ‘follow the data.’⁶⁰ Doing so reveals how collaborations and interdependencies are exercised, maintained, and amplified in data infrastructures, throughout access networks, backbone systems, applications, and data services.⁶¹

Applying this lens to Palestine allows us to trace how voice communications move from ordinary conversations into the hands of a web of surveillance actors, the relationships between which are visually represented in the map below, and investigated in more detail in the following sections.

56 Al Jazeera, ‘What Is Project Nimbus, and Why Are Google Workers Protesting Israel Deal?’, Al Jazeera, 23 April 2024, <https://www.aljazeera.com/news/2024/4/23/what-is-project-nimbus-and-why-are-google-workers-protesting-israel-deal>.

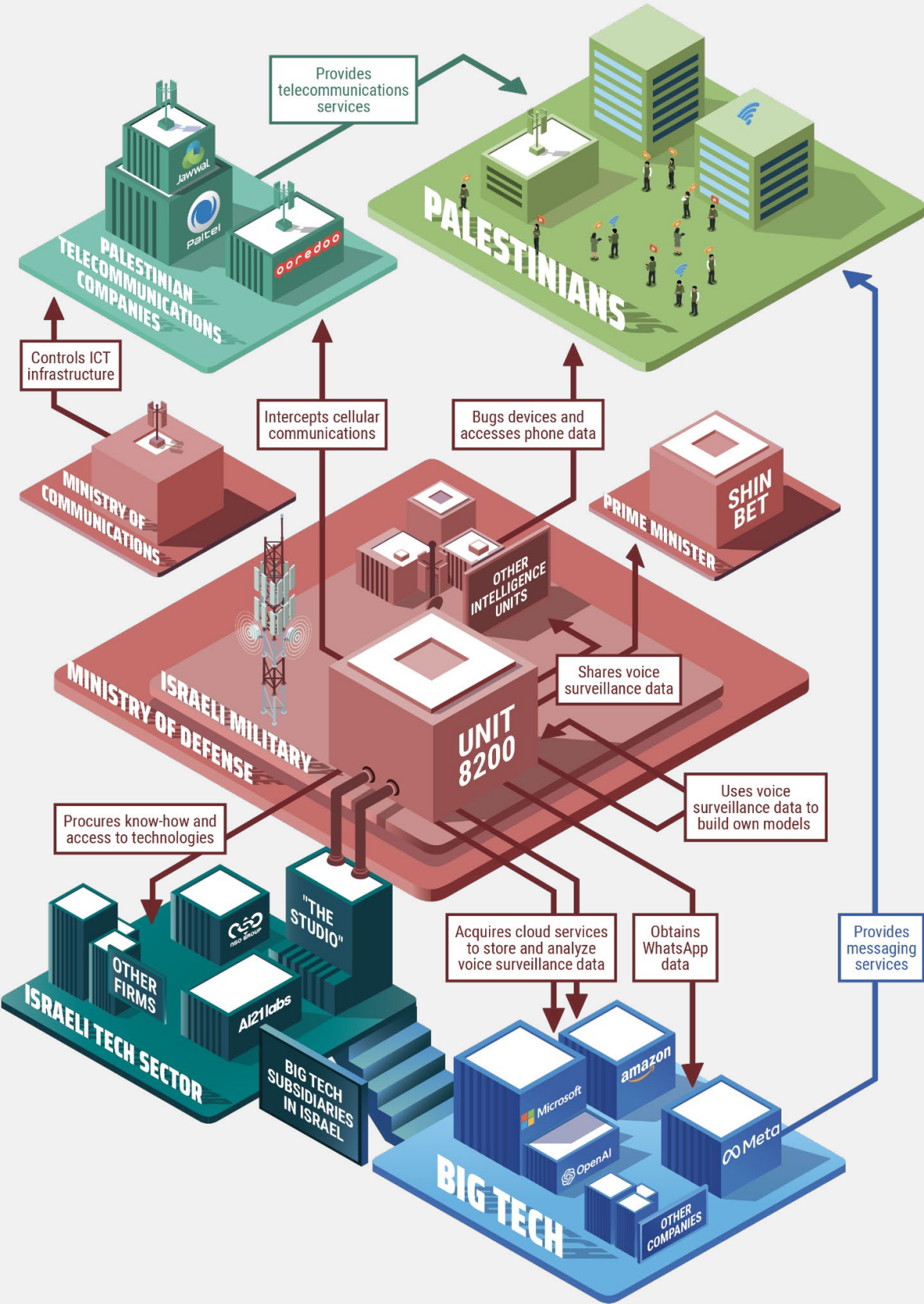
57 Investigate, ‘Amazon.Com Inc.’, The American Friends Service Committee, 7 August 2024, <https://investigate.info/company/amazon>; Investigate, ‘Microsoft Corp.’, The American Friends Service Committee, 29 January 2025, <https://investigate.info/company/microsoft>.

58 Danny O’Brien and Jillian C. York, ‘A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?’, Electronic Frontier Foundation, 11 November 2015, <https://www.eff.org/deeplinks/2015/11/palestine-3g>.

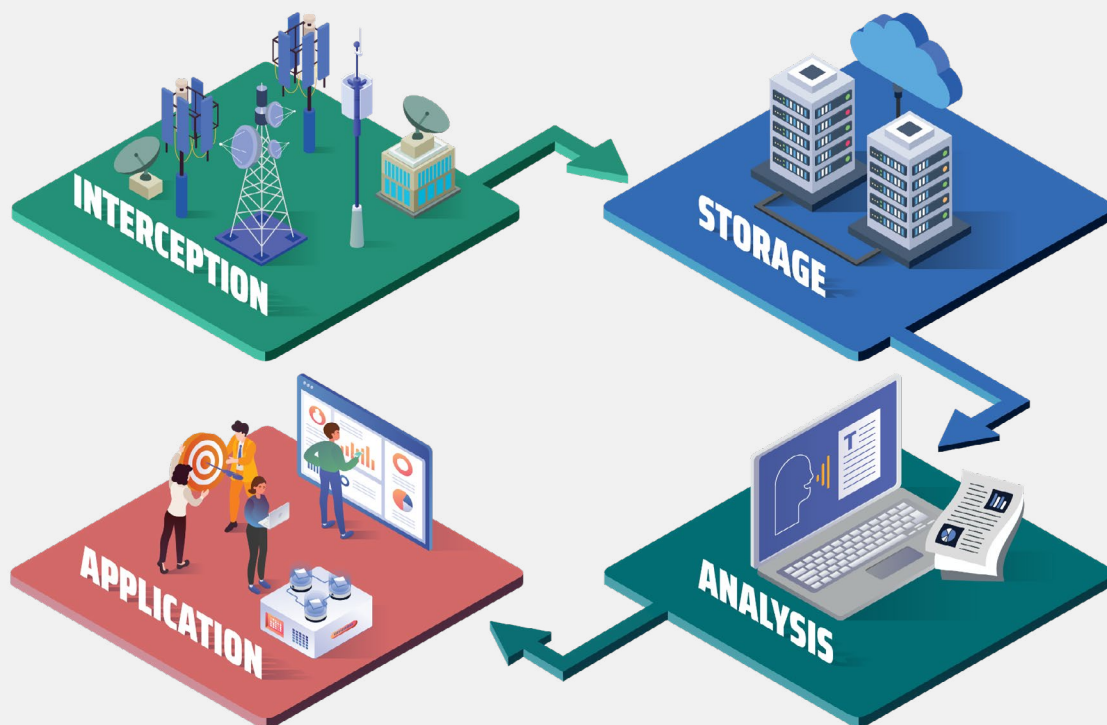
59 Oslo Accords, Annex III, Concerning Civil Affairs, Israeli Palestinian Interim Agreement on The West Bank and the Gaza Strip (Oslo II) (1995), 35–36, https://www.peaceagreements.org/media/documents/ag985_56017411a3c68.pdf.

60 Flensburg and Lai, ‘Follow the Data! A Strategy for Tracing Infrastructural Power’, 319.

61 Flensburg and Lai, ‘Follow the Data! A Strategy for Tracing Infrastructural Power’, 319–20.



Following the voice-surveillance data, this report is structured along four steps: the interception of communications and voice data capture (Section 2), the storage and retention of voice-surveillance data (Section 3), the processing and analysis of voice-surveillance data (Section 4), and the applications for voice-surveillance data (Section 5). While presented sequentially, these steps are part of a continuous and iterative process, paradigmatic of data infrastructures.



2. INTERCEPTION AND CAPTURE OF VOICE DATA

2.1. PALESTINIANS UNDER VOICE SURVEILLANCE

What began as targeted monitoring of select individuals has expanded into a population-wide voice-surveillance regime. This section describes the current scope of voice surveillance in Palestine, the groups it singles out for closer scrutiny, and its expanding geographic reach.

Mass surveillance of every Palestinian

Israeli voice surveillance of Palestinians today operates at a mass scale, targeting everyone. Journalist Lubna Masarwa in Middle East Eye reported in 2021 that “Israel can listen to any conversation in the West Bank and the Gaza Strip,”⁶² elaborating that, “[a]t any given time, hundreds of soldiers are listening to the conversations being conducted.”⁶³ While this article was new to a more English-speaking (and international) readership, years prior in

62 Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’.

63 Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’.

2014, Waji Al-Jaafari in Ma'an News Agency referenced Palestinian officials who reported that Israel monitors all means of communication in Palestine, including through mobile phones and landlines.⁶⁴ For instance, Suleiman al-Zuhairi, Undersecretary of the Ministry of Communications and Information Technology, spoke about Unit 8200's apparatus of electronic espionage used for intercepting, among other things, telephone calls.⁶⁵

This ability to surveil every Palestinian, rather than select targets, is enabled by increased access to cloud storage and cloud computing usage. As part of a 2025 investigation of Israel's "ambitious project to store a giant trove of Palestinians' phone calls on Microsoft servers in Europe," The Guardian called this surveillance system "indiscriminate," allowing "intelligence officers to play back the content of cellular calls made by Palestinians, capturing the conversations of a much larger pool of ordinary civilians."⁶⁶ Whereas, before these partnerships with cloud computing giants, the Israeli military was only able to store "the calls of tens of thousands of Palestinians" that were pre-determined as surveillance targets, and did so on its own internal servers.⁶⁷ With access to cloud storage, the Israeli military no longer needed to limit itself to who should be targeted for surveillance.⁶⁸

Particular target groups of interest

That said, within the broader Palestinian population, the same 2021 Middle East Eye article named two categories of individuals as being of particular interest to Israel's military and internal security agencies. These include: (1) Palestinians who are politically active, and (2) individuals whose personal circumstances make them vulnerable to blackmail. These groups of interest build on long-standing precedents. More than a decade ago, veterans of Unit 8200 acknowledged monitoring Palestinian civilians in order to gather sensitive personal information for potential leverage, and also "admitted to tracking political activists."⁶⁹

When it comes to the former group, a human rights lawyer described how the Shin Bet is "particularly bothered by nonviolent activists, because such people can lead a popular movement and generate widespread protest."⁷⁰ In his view, "what worries them most is civil society organisations, because they could lead to the end of the occupation and they garner sympathy in the international community."⁷¹ Surveilling politically active Palestinians is central to Israel's resistance suppression aims.

64 Wajdi Al-Jaafari, "Masūlūn: jamy' wasā'il al'ittiḥāl fi falasṭīn murāqaba" [Officials: All means of communication in Palestine are monitored], Ma'an News Agency, 20 December 2014, <https://www.maannews.net/news/748592.html>.

65 Al-Jaafari, "Masūlūn: jamy' wasā'il al'ittiḥāl fi falasṭīn murāqaba" [Officials: All means of communication in Palestine are monitored].

66 Harry Davies and Yuval Abraham, "A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians', The Guardian, 6 August 2025, <https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud>.

67 Davies and Abraham, "A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

68 Abraham, 'Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians'.

69 Yuval Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians', +972 Magazine, 6 March 2025, <https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/>.

70 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

71 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

As for the latter group, whom an Israeli army veteran called “pressure points,” it includes people whom or whose family members—for their sexual orientation, illnesses, indebtedness, or other circumstances—are forced by the Shin Bet “to collaborate or reveal things about other people,” as a practice of control and intimidation.⁷²

Geographic focus and expansion

Geographically speaking, voice surveillance initially focused on the Palestinian population of the West Bank. In recent years, the system expanded to cover Gaza as well.⁷³ After October 2023, an intelligence officer explained to +972 Magazine that “internal enthusiasm for storing mass surveillance data from Gaza on the cloud-based system increased,” stating that the goal was to head “toward long-term control there, like in the West Bank.”⁷⁴ However, sources expressed to The Guardian their concerns about how this voice-surveillance project might be impacted by the destruction of the telecommunications infrastructure in Gaza,⁷⁵ which “has reduced the volume of phone calls in the territory.”⁷⁶

The expansion from targeted to population-wide voice surveillance, its geographic extension from the West Bank to include Gaza as well, and the vastly increased collection capacity afforded by cloud infrastructure raise critical questions about what forms of data are being captured.

2.2. DATA CAPTURED

Audio recordings of conversations

Available reporting indicates that the system archives recordings of calls made daily by Palestinians, in the form of audio files—not just textual data,⁷⁷ archiving “millions of mobile phone calls made each day by Palestinians in Gaza and the West Bank.”⁷⁸ These intercepted audio recordings constitute the core of the voice-surveillance repository.

Corresponding metadata

In addition to audio files, the system collects the corresponding metadata linked to each call. While audio files reveal what is being said, metadata gives information about phone call participants, time, as well as contacts and location.⁷⁹

72 Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’.

73 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

74 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

75 Mohammed Alshurafa, The Impact of the Gaza Blockade and the Destruction of Telecommunications Infrastructure on the Digital Economy Amidst Genocide (7amleh – The Arab Center for the Advancement of Social Media, 2025), <https://7amleh.org/post/gaza-digital-economy-collapse-en>; 7amleh, Gaza Telecommunications Infrastructure: Assessment to Damages and Humanitarian Impact (7amleh – The Arab Center for the Advancement of Social Media, 2024), <https://7amleh.org/post/impact-of-war-on-gaza-s-telecommunications-infrastructure-en>.

76 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

77 Yuval Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War”, +972 Magazine, 4 August 2024, <https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/>; Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’; Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

78 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

79 Robin James, ‘Acousmatic Surveillance and Big Data’, Sounding Out!, 20 October 2014, <https://soundstudiesblog.com/2014/10/20/the-acousmatic-era-of-surveillance/>.

Voice-surveillance metadata extracted alongside phone calls most likely include the time and duration of the call, the date and time stamps, the source and destination of the call, the participants in the call, the owner of the device or SIM card associated with the call, and more. As described in one report in *The Guardian*, “intercepted phone calls tied to a person’s profile [...] include the time the person called and the names and numbers of those on the call.”⁸⁰

Even though metadata provides mainly contextual information around the voice conversation, a lot can be surmised from it about the content of the conversation as well. Lawyer Usama Halabi illustrates this point through an example, stating that, for instance, if the metadata reveals “that a journalist called a certain source, it may be possible to ascertain to a significant degree the content of the call from the mere fact that it was made.”⁸¹

Potential WhatsApp-related data

Reports that surfaced in 2024 hypothesized that the data captured by the voice-surveillance regime may extend beyond traditional telecom calls to include information associated with WhatsApp communications.⁸² Observers have raised the possibility that Israel is collecting WhatsApp-related data, though it remains unclear whether this includes only metadata or also the content of communications such as voice notes and in-app call recordings. If accurate, these reports would suggest an even broader sweep of captured data, encompassing both telecom network activity and app-based voice exchanges.

2.3. INTERCEPTION METHODS

Israel’s voice surveillance of Palestinians relies on multiple interception methods that draw on both direct access to telecommunications infrastructure and the compromise of individual devices. Two mechanisms—bugging phones and monitoring ICT networks serving the occupied territories—are well documented. A third, still unconfirmed, concerns the possible interception of data from encrypted messaging applications such as WhatsApp.

Compromising devices through implanted bugs and spyware

One confirmed interception method for voice-surveillance data involves the physical compromise of mobile phones entering Gaza. A former signals intelligence member told *Middle East Eye* in 2021 that “[e]very mobile or phone imported into Gaza through the Kerem Shalom crossing [...] is implanted with an Israeli bug.”⁸³ The use of the term ‘implanted’ suggests a hardware-based mechanism rather than software-based spyware, indicating the insertion of an electronic component that can transform the phone into

80 Michael Biesecker et al., ‘As Israel Uses US-Made AI Models in War, Concerns Arise about Tech’s Role in Who Lives and Who Dies’, *AP News* (Tel Aviv), 18 February 2025, <https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108>.

81 Halabi, ‘Legal Analysis and Critique of Some Surveillance Methods Used by Israel’, 215.

82 Sada Social, Sada Social Calls for Immediate Investigation into Meta’s Leak of WhatsApp Users’ Data to the Israeli Military, 18 May 2024, <https://sada.social/post/sd-soshal-ydaao-l-thkyk-aaagl-ofory-ltsryb-myta-byanat-mstkhdm-y-oatsab-l-algysh-alsrayly>; Rabia Ali, ‘Is WhatsApp Putting Palestinians at Risk of Being Killed in Gaza?’, *Anadolu*, 30 April 2024, <https://www.aa.com.tr/en/artificial-intelligence/is-whatsapp-putting-palestinians-at-risk-of-being-killed-in-gaza/3206563>; Paul Biggar, Meta and Lavender, 16 April 2024, <https://blog.paulbiggar.com/meta-and-lavender/>.

83 Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’.

a listening device. This interpretation aligns with earlier statements from former Minister of Communications Masshour Abu Daqqa, who noted in 2014 that Israel prevented the entry of devices—particularly some Chinese equipment—that it found difficult to hack or eavesdrop on,⁸⁴ further substantiating the use of hardware-based interception.

Phones can also be compromised through spyware, which can covertly activate a device's microphone and access a broad range of data. One of the most widely known examples is NSO Group ("NSO")'s Pegasus software. Human Rights Watch describes Pegasus as able to turn a phone "into a portable surveillance tool by gaining access to the phone's camera, microphone, and text messages."⁸⁵ One instance of the use of Pegasus on Palestinians was corroborated by technical research conducted in 2021 by Front Line Defenders.⁸⁶ Their research was later independently peer reviewed by the University of Toronto's Citizen Lab and Amnesty International's Security Lab, who performed forensic analysis and concluded "that the devices of six Palestinian human rights defenders were hacked with NSO's Pegasus spyware in 2020 and 2021."⁸⁷

Controlling telecommunications infrastructure

A second confirmed interception mechanism derives from Israel's structural control over Palestinian telecommunications networks, previously delineated in Section 1. As one source explained to Middle East Eye, "anyone using the only two mobile networks serving the occupied territories [Jawwal and Wataniya—now Ooredoo Palestine] is being monitored."⁸⁸

The Electronic Frontier Foundation noted in 2015 that Israel had restricted Palestinian operators, locking them down to older generations of mobile technology that is "more vulnerable to being tapped," and blocking access to newer systems that "are safer from passive surveillance,"⁸⁹ enabling Israel to "surveil and eavesdrop [...] on traffic coming over Israeli companies' networks" without being detected.⁹⁰ Without this level of control, Israel would need to resort to more active modes of surveillance, such as using spying technology like IMSI (International Mobile Subscriber Identity) catchers. However, unlike passive surveillance, active surveillance is more detectable.

Possibly accessing WhatsApp communications

A further, though still unresolved, question concerns whether Israel can access communications conducted via WhatsApp, the contents of which are presumably encrypted. Reports by +972 Magazine and Local Call, citing

84 Al-Jaafari, "Masūlūn: jamy' wasā'il al'ittiḍāl fi falasṭīn murāqaba" [Officials: All means of communication in Palestine are monitored].

85 Human Rights Watch, Spyware Used to Hack Palestinian Rights Defenders, 8 November 2021, <https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders>.

86 Front Line Defenders, OPT/Israel: Six Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware (Front Line Defenders, 2021), <https://www.frontlinedefenders.org/en/statement-report/six-palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware>.

87 Amnesty International, Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware, 8 November 2021, <https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/>.

88 Masarwa, 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'.

89 O'Brien and York, 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?'

90 O'Brien and York, 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?'

six Israeli intelligence officers, claim that conversations between Palestinians on WhatsApp have been used to feed Israel's target-generation system, Lavender. The reporting prompted questions from observers, including Tech for Palestine founder Paul Biggar, who asked, "Where are they getting this data? Is WhatsApp sharing it?"⁹¹ On their end, a WhatsApp spokesperson denied that the company provided a backdoor or "bulk information" to any government, implying Israel as well.⁹² Nonetheless, a 2024 press release by civil society organization Sada Social Center admonished Meta for what they considered to be a "leak of Palestinian data" that includes their communications via WhatsApp.⁹³ However, some have suggested that Israel might have obtained WhatsApp data through methods other than backdoor access or a leak. Journalist Marc Owen Jones suggested Israel could gain access to WhatsApp data through other means, such as through informants, hacking, or spyware.⁹⁴ This is not a far-fetched hypothesis, seeing as, in October 2025, a United States (U.S.) judge granted Meta an injunction to stop NSO's spyware from targeting WhatsApp users, particularly journalists, lawyers, and human rights activists,⁹⁵ an injunction NSO has since sought to overturn.⁹⁶ Additionally, other experts like activist Esra'a Al Shafei posited that Israel may have access to "the metadata alone," which, still, would reveal group memberships, contact networks, and communication patterns but not conversation content.⁹⁷

3. VOICE DATA STORAGE AND RETENTION

Israel's mass interception of Palestinian voice communications relies on a layered storage architecture supported by major cloud providers and flexible retention practices. Large volumes of audio recordings and associated metadata are housed across Microsoft Azure and Amazon Web Services (AWS) environments, seemingly both inside Israel and in data centers abroad, reflecting the scale of surveillance and the military's reliance on commercial cloud infrastructure.

3.1. CLOUD STORAGE AND PROVIDERS

The scale and scope of Israel's voice surveillance of Palestinians has made reliance on commercial cloud providers essential. The volume of data—comprising billions of audio files and associated metadata—exceeds what could reasonably be stored on military servers alone. As a result, much of the intercepted voice data is hosted in the cloud, primarily through Microsoft

91 Biggar, Meta and Lavender.

92 Ali, 'Is WhatsApp Putting Palestinians at Risk of Being Killed in Gaza?'

93 Sada Social, Sada Social Calls for Immediate Investigation into Meta's Leak of WhatsApp Users' Data to the Israeli Military.

94 Marc Owen [@marcownjones] Jones, 'The question about Lavender using Whatsapp groups for their targeting, and Meta's potential role in this is important', 17 April 2024, https://x.com/marcownjones/status/1780501998728540589?ref_src=twsrc%5Etfw.

95 Al Jazeera, 'US Court Bars Israeli Spyware Firm from Targeting WhatsApp Users', Al Jazeera, 18 October 2025, <https://www.aljazeera.com/news/2025/10/18/us-court-bars-israeli-spyware-firm-from-targeting-whatsapp-users>.

96 Suzanne Smalley, 'NSO Seeks to Overturn WhatsApp Case, Saying It Is "Catastrophic" for the Spyware Maker', The Record, 20 November 2025, <https://therecord.media/nso-seeks-to-overturn-whatsapp-case>.

97 Julia Conley, 'Report Indicates Israel Uses WhatsApp Data in Targeted Killings of Palestinians', Truthout, 19 May 2024, <https://truthout.org/articles/report-indicates-israel-uses-whatsapp-data-in-targeted-killings-of-palestinians/>.

Azure and AWS, with some data reportedly still retained on Israeli military servers, though details about domestic storage remain limited.

Microsoft Azure

Investigations in 2025 by The Guardian, +972 Magazine, and Local Call, drawing on leaked Microsoft documents and interviews with nearly a dozen sources from Microsoft and the Israeli military, revealed that Unit 8200 transferred recordings of Palestinian calls to a “customized and segregated area within Microsoft’s Azure cloud platform.”⁹⁸ This includes voice data from the population of Gaza.⁹⁹ The setup of this cloud environment was the result of a close collaboration between Microsoft engineers and Unit 8200, beginning as early as 2022, aiming to create a system “carefully tailored to the unit’s needs.”¹⁰⁰ Some Microsoft employees involved were themselves former Unit 8200 members, a factor described by sources as making the collaboration “much easier.”¹⁰¹ This collaboration forms part of a broader, privileged partnership between Microsoft and Israel, with the tech giant being examined as having a “footprint in all major military infrastructures in Israel.”¹⁰²

Amazon Web Services

In addition to Microsoft, Amazon also provides cloud storage for Israeli voice-surveillance data. Another investigation by +972 Magazine and Local Call reported that AWS hosts data collected through the mass surveillance of Gaza’s population, including billions of audio files.¹⁰³ It is unclear whether this storage is part of Project Nimbus—the \$1.3 billion joint cloud and artificial intelligence contract signed by Google and Amazon with the Israeli government and military in 2021—though it is known that the majority of purchases from Amazon and Google are carried out through said contract. Similarly to Microsoft, Amazon is, too, considered to have a close partnership with Israel, providing “Israel’s Military Intelligence Directorate with a server farm which is used to store masses of intelligence information.”¹⁰⁴

Publicly available reports on Amazon’s role seems to indicate that its storing of voice-surveillance data is more focused on the people of Gaza, as said reports do not explicitly mention the West Bank or occupied East Jerusalem. According to multiple sources, the AWS public cloud system allows the Israeli military to have “endless storage” for holding intelligence on almost ‘everyone’ in Gaza.¹⁰⁵ Although the system had been in use since the end of 2022, its operational role expanded significantly after October 2023.¹⁰⁶

98 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

99 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

100 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

101 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

102 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

103 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War’.

104 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War’.

105 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War’.

106 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War’.

Reliance on Big Tech's cloud infrastructure

Israeli military sources acknowledge that the scale of its voice-surveillance architecture necessitates reliance on Big Tech cloud providers, as it “is so large that it cannot be stored on military servers alone.”¹⁰⁷ In the words of the officer in charge of Israel’s Digital Transformation Administration in a 2020 interview, “[t]he army can’t compete with the resources that the cloud giants and the rest of the cloud providers invest in building their cloud, so it’s useless to even try and compete with them.”¹⁰⁸ For this reason, Unit 8200 leadership concluded that Azure’s “near-limitless storage capacity” was essential to store the communications of an entire population, and had ambitions to expand this operation significantly—to the tune of “tenfold in the coming years.”¹⁰⁹

3.2. LOCATION OF DATA CENTERS AND SERVERS

Recent reporting has shed light on the geographic distribution of the infrastructure used to store Israel’s voice-surveillance data on Palestinians. A significant portion of this data—amounting to thousands of terabytes—has been held outside Israel, primarily in Microsoft Azure data centers located in Europe.

European data centers

According to a joint investigation by The Guardian, +972 Magazine, and Local Call, “leaked Microsoft files suggest that a large proportion of the unit’s sensitive data may now be sitting in the company’s datacentres in the Netherlands and Ireland.”¹¹⁰ By July 2025, Microsoft’s Azure facility—a 14-hectare data-center campus near Middenmeer in North Holland—was reportedly hosting 11,500 terabytes of Israeli military data, described as roughly 200 million hours of audio files.¹¹¹ In another report by the same investigative team, the volume was cited as “as much as 8,000 terabytes of data,”¹¹² reflecting some variation in publicly available estimates but still highlighting the immense scale of the voice data stored.

Ireland served as an additional European hub, which is not surprising given that it is home to Microsoft’s European headquarters.¹¹³ Although exact figures were not disclosed, reporting indicates that a “smaller proportion” of the total data—relative to the volume held in the Netherlands—was stored in Microsoft Azure servers there.¹¹⁴

107 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War’.

108 Josh Mitnick, ‘Here’s How the Israeli Army Is Embracing Digital Transformation’, CIO, 8 February 2020.

109 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

110 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

111 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

112 Harry Davies and Yuval Abraham, ‘Microsoft Blocks Israel’s Use of Its Technology in Mass Surveillance of Palestinians’, The Guardian, 25 September 2025, <https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians>.

113 Lisa O’Carroll, ‘Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF’, The Guardian, 4 December 2025, <https://www.theguardian.com/technology/2025/dec/04/irish-authorities-asked-to-investigate-microsoft-over-alleged-unlawful-data-processing-by-idf>.

114 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

Rapid data relocation after public exposure

Following publication of the joint investigation detailing these arrangements, Unit 8200 appears to have moved quickly to extract its voice-surveillance archives from at least one European Union (EU) jurisdiction. According to sources familiar with the transfer, the data was relocated “within days,” with the move occurring in early August 2025. Intelligence officials suggested that the data was likely being transferred to Amazon Web Services (AWS), which was not confirmed by either Israel’s military nor Amazon.¹¹⁵

Storage within Israel

In contrast to the details emerging from reporting on European infrastructure, the location and scale of servers inside Israel remain far less visible. Prior to its migration to the cloud, Unit 8200 stored only the calls of those pre-designated as surveillance ‘suspects’ on its own internal servers.¹¹⁶ Even before the decision to shift storage from Microsoft’s servers in the Netherlands, Unit 8200 allegedly planned to migrate as much as 70% of its voice-surveillance data to Azure,¹¹⁷ suggesting that at least some of the voice data repository would remain under the unit’s storage infrastructure.

It is unclear whether this residual data resides on the military’s own servers or in facilities operated within Israel by Microsoft and Amazon. Both companies have expanded their data center infrastructure in the past several years, with Microsoft launching a datacenter region in Israel in 2020¹¹⁸ and Amazon in 2023.¹¹⁹ Even so, public sources do not clarify where voice-surveillance data is stored inside Israel.

3.3. DATA RETENTION PERIODS

Israel’s retention of intercepted Palestinian voice data remains flexible in practice. According to intelligence sources cited in recent investigations, recorded calls—including those made to international and Israeli numbers—are “typically retained in the cloud for about one month” in the case of Microsoft Azure.¹²⁰ However, these same sources emphasized that the retention period can be extended on demand, enabling Unit 8200 to preserve recordings for significantly longer periods “when needed.”¹²¹ The Azure-based storage and processing environment is designed to allow officers to “play back and analyse the content of cellular calls of an entire population.”¹²² This means that intelligence officers can retroactively retrieve the conversations of individuals who later become “of interest,” effectively transforming a month-long retention policy into a selective long-term

115 Davies and Abraham, ‘Microsoft Blocks Israel’s Use of Its Technology in Mass Surveillance of Palestinians’.

116 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

117 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

118 Microsoft, Microsoft to Launch New Cloud Data Center Region in Israel, 22 January 2020, <https://news.microsoft.com/source/emea/features/microsoft-to-launch-new-cloud-datacenter-region-in-israel/>.

119 Dan Swinhoe, AWS Launches Israeli Cloud Region in Tel Aviv, 2 August 2023.

120 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

121 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

122 Davies and Abraham, ‘Microsoft Blocks Israel’s Use of Its Technology in Mass Surveillance of Palestinians’.

archive.¹²³ No publicly available information exists on the retention periods for voice-surveillance data stored in Amazon AWS.

4. VOICE DATA PROCESSING AND ANALYSIS

This section details the algorithmic tools likely used to process and analyze voice-surveillance data, specifically to identify speakers, transcribe and translate recorded audio, and analyze the contents of speech.

4.1. SPEAKER IDENTIFICATION

In simplified terms, Israel's ability to identify individuals participating in intercepted calls is likely grounded in two broad methods of speaker identification: metadata-based inference and biometric voiceprinting. Both approaches are not mutually exclusive.

Metadata-based inference

The first method relies on information obtained from telecommunications metadata, particularly the SIM cards used to place or receive a call. By linking the SIM ID to subscriber records, authorities can narrow the pool of likely speakers to the card owner and their immediate family or social network. Even when the speaker is not the registered owner, patterns in their networks and contact lists may allow analysts to deduce who is using the device at any given moment. This method was referenced in an AP News article detailing that intercepted calls “tied to a person’s profile also include the time the person called and the names and numbers of those on the call.”¹²⁴

Biometric voiceprinting

The second method, voiceprinting, is a biometric technique that derives a unique vocal signature from an individual’s physiological characteristic (e.g., vocal tract shape, glottis, nasal cavity) and behavioural speech patterns (e.g., accent, pitch, speaking style). Researchers at the Palestine Polytechnic University note that voiceprinting has distinct advantages over other biometric modalities, explaining that, a “voiceprint does not require special hardware like a fingerprint sensor or iris-scanning equipment, it just requires a microphone which is cheap and easy to get.”¹²⁵ Microphones, especially those built in mobile phones, don’t even need to be acquired by Israel.

Several recent commentaries—primarily opinion pieces—assert that Israel is deploying voiceprinting at scale. Articles in *Al Majalla* by foreign-policy analyst Marco Mossad claim that the Israeli military created a “voice

123 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

124 Biesecker et al., ‘As Israel Uses US-Made AI Models in War, Concerns Arise about Tech’s Role in Who Lives and Who Dies’, 18 February 2025.

125 Mohamad Ateyyah Salah et al., ‘Voiceprint Authentication System’ (Palestine Polytechnic University, 2021), <https://scholar.ppu.edu/bitstream/handle/123456789/7547/Voiceprint-Authentication-System.pdf>.

library,”¹²⁶ and tracked militants’ calls “through their phones, listened to their calls with relatives and family members, and then recorded each voice, creating their unique voiceprints in databases,”¹²⁷ allegedly enabling rapid identification during eavesdropping operations. Similar assertions are made in *The Peninsula* by cyber-politics researcher Khaled Walid Mahmoud, who describes “massive voice libraries” used to match newly intercepted audio against stored profiles and suggests that system accuracy increases as more calls are captured.¹²⁸ Retired Major General Fayez al-Duwairi, in *Al Jazeera*, further contended that Israel collected the voices of approximately 37,000 individuals at the outset of its recent military campaign in Gaza.¹²⁹

Although these accounts provide a consistent narrative, they do not offer verifiable sourcing. Earlier reporting, however, indicates that such capabilities have been discussed within Palestinian media for over a decade. In 2013, *Palestine Today* cited security researcher Samir Mahmoud Qaddih who described the use of voiceprints by Israel after tapping the phone calls and tracing the full call histories of targeted individuals and their contacts.¹³⁰ *Al-Monitor* (2014)¹³¹ and *Rai Al-Youm* (2016) echoed these claims, with the latter adding that device microphones could allegedly capture sound even when phones were switched off,¹³² something advanced spyware can achieve by simulating a power-off state to deceive the user while the device remains turned on and under malicious control.¹³³

Unresolved questions about technology providers

On the one hand, speaker identification through metadata is likely done by Israeli intelligence units, using data captured through the monitoring of cellular networks, potentially in collaboration with the Israeli Ministry of Communications. This hypothesis is an educated guess.

On the other hand, despite the recurring references to voiceprinting, publicly available information does not clarify whether these systems are developed in-house by the Israeli military, procured from domestic private contractors, or sourced from international vendors. Israel’s private sector includes

126 Marco Mossad, ‘Are Global Tech Giants Facilitating Israel’s War on Gaza?’, *Al Majalla*, 31 May 2024, <https://en.majalla.com/node/318176/science-technology/are-global-tech-giants-facilitating-israel%E2%80%99s-war-gaza>.

127 Marco Mossad, ‘Voiceprint Technology: A Commercial Hit with Military Utility’, *Al Majalla*, 7 February 2024, <https://en.majalla.com/node/310146/science-technology/voiceprint-technology-commercial-hit-military-utility>.

128 Khalid Walid Mahmoud, ‘Voiceprint: From a Verification Tool to a Tracking Technology’, *The Peninsula*, 19 January 2025, <https://thepeninsulaqatar.com/opinion/19/01/2025/voiceprint-from-a-verification-tool-to-a-tracking-technology>.

129 *Al Jazeera*, ‘Al-Duwairi: Al-Āṭilāl Yastūdim BaḌmaṭ al-Ḍūt WālḌin LitḌqwb Muqāṭilī al-Muqāwama Biḡaza بصمة الاحتلال يستخدم بصمة Biḡaza الدويري: الاحتلال يستخدم بصمة Biḡaza للصوت والعين لتعقب مقاتلي المقاومة بغزة [Al-Duwairi: The Occupation Uses Voice and Eye Scans to Track Resistance Fighters in Gaza]’, *Al Jazeera*, 15 April 2025, <https://www.aljazeera.net/news/الدويري-الاحتلال-يستخدم-بصمة-الصوت>.

130 *Palestine Today*, “‘Kayfa tatanaḌat almuḌabarāt al’isrā’īlya Ḍalā jawwālik āṣaḌsy!’؟ كيف تنتصت المخابرات الإسرائيلية على جوالك الشخصي؟ [How does Israeli intelligence eavesdrop on your personal mobile phone?!]”, *Palestine Today*, 30 December 2013, <https://paltodaytv.com/post/466/كيف-تنتصت-المخابرات-الإسرائيلية-على-جوالك-الشخصي>.

131 Hana Salah, “‘AlbaḌma as-Ḍaūtya’ Adāt Isrā’īl Litanfīl Syāsāt ‘AttaḌafya al-Jasadya’ البصمة الصوتية أداة إسرائيل لتنفيذ سياسة “التصفية” [“Voiceprints”: Israel’s Tool for Implementing “Elimination”]’, *Al-Monitor*, 4 February 2014, <https://www.al-monitor.com/ar/contents/articles/originals/2014/02/gaza-israel-islamic-jihad-hamas-mobile-war.html>.

132 Yassin Jamil, “‘TafāḌil MuḌhila Ḍan Ḍuruq Wa Ḍasālīb al-Murāqaba as-Sirrya al-Isrā’īlya Lil-Hawātīf al-Jawwāla Lil-Muqāwama al-Filsṭīnya Wal-Lubnānya’ تفصيل مذهلة عن طرق وأساليب المراقبة السرية الإسرائيلية للهواتف الجواله للمقاومة الفلسطينية واللبنانية [Shocking Details Emerge about Israel’s Covert Methods and Techniques for Monitoring the Mobile Phones of the Palestinian and Lebanese Resistance]”, *Rai Alyoum*, 21 June 2016, <https://www.raialyoum.com/ل-تفاصيل-مذهلة-عن-طرق-وأساليب-المراقبة>.

133 AVG, Malware Is Still Spying on You Even When Your Mobile Is Off, 14 September 2018, <https://www.avg.com/en/signal/android-spyware-that-works-when-your-phone-is-off>.

a plethora of companies with advanced audio-analysis capabilities, and Unit 8200 is known to incubate its own technologies. Thus, the provenance of speaker-identification tools remains an open question.

4.2. SPEECH TRANSCRIPTION AND TRANSLATION

Israel's voice-surveillance system necessitates large-scale speech transcription and translation. The first process, speech transcription, is technically referred to as automatic speech recognition (ASR) or speech-to-text (STT)—the two having subtle differences that are not of major relevance for this report and are often used interchangeably. The second process, speech translation, is distinct from speech transcription. However, most available sources discuss them together, and for the purposes of this report, they are therefore treated as a combined set of capabilities for converting spoken Arabic into searchable, analyzable text.

From manual to automated transcription

Historically, intercepted conversations were transcribed manually. Former soldiers have described how Jewish Israeli soldiers who studied Arabic were tasked with listening to recorded calls and producing transcripts.¹³⁴ Their work was reviewed by Druze soldiers or Jewish soldiers of Syrian descent, “for whom Arabic is their mother tongue,”¹³⁵ as most military officers admitted in testimonials that their level of Arabic is “basically zero.”¹³⁶ Given, again, the scale of voice-surveillance data being captured by Israel, the processes of transcription and translation are now relying on automated systems.

Rationale for the integration of cloud-based transcription tools

The use of Microsoft Azure's models—along with those of other cloud companies—is accompanied or is potentially supplanting Unit 8200's own “smaller language models” capable of transcribing and translating spoken Arabic to Hebrew.¹³⁷ A +972 Magazine recalled internal discussions around cloud migration, explaining that commanders emphasised the advantage of leveraging built-in cloud services once their data is migrated to the cloud, as the cloud service providers “also have their own STT [speech-to-text] capabilities. These are good; they have many capabilities. Why develop everything in the army unit if the capabilities already exist?”¹³⁸

Experts of algorithmic supply chains explain how this is part of the *modus operandi* of cloud providers. Such companies, as is the case for Microsoft, offer their own pre-built AI technologies as a service “in areas such as language, speech, [...] and analytics,” alongside their cloud storage capabilities.¹³⁹ Only a limited number of organizations “can produce bespoke

134 Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’.

135 Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’.

136 Breaking the Silence, Military Rule: Testimonies of Soldiers from the Civil Administration, Gaza DCL and COGAT (Breaking the Silence, 2022), 41, https://www.breakingthesilence.org.il/inside/wp-content/uploads/2022/07/Military_rule_testimony_booklet.pdf.

137 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War’.

138 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War’.

139 Jennifer Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 2023 ACM Conference on Fairness Accountability and Transparency, 12 June 2023, 1188, <https://doi.org/10.1145/3593013.3594073>.

state-of-the-art AI technologies in-house.”¹⁴⁰ This is because of significant barriers to entry, including access to “large and relevant quantities of data, potentially from multiple sources and labelled or moderated, relating to many use-cases, contexts, and subjects” as well as “scarce expertise in model training, testing and deployment, all with significant storage, compute, and networking needs.”¹⁴¹ As such, major companies like Microsoft and Amazon offer cloud-based AI technologies to “strategically position themselves in markets and supply chains of many kinds.”¹⁴²

Use of Amazon and Microsoft’s pre-built transcription and translation functions

For the voice data stored in AWS, publicly available information does not confirm the use of its tools for transcription and translation. However, considering the abovementioned barriers to entry, it is quite possible that Unit 8200 uses Amazon Transcribe¹⁴³ and Amazon Translate¹⁴⁴ for the voice-surveillance data it stores on AWS.

For the data stored by Microsoft, AP News revealed that Israel uses Azure tools for the transcription and translation of “phone calls [...] and audio messages” stored in the company’s cloud.¹⁴⁵ While the specific tools are not enumerated in leaked documents reviewed by The Guardian, their report also indicates “use by the Israeli military of Azure’s “AI-powered translation and speech-to-text conversion tools,”¹⁴⁶ with translation accounting for “about half of the average monthly consumption.”¹⁴⁷

These features match the description of Microsoft’s Azure Speech, which, according to its website, include speech-to-text, including the transcription of pre-recorded audio files as well as the batch transcription of large volumes of audio.¹⁴⁸ Other features of relevance comprise language identification, pronunciation assessment, and speech translation.¹⁴⁹ Given these capabilities—and the Israeli military’s substantial AI consumption through Azure—there are reasonable grounds to conclude that Azure Speech services are used to process the voice data hosted in the Azure cloud.

140 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1188.

141 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1188.

142 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1189.

143 Amazon Web Services, Speech to Text Service - Amazon Transcribe, n.d., <https://aws.amazon.com/pm/transcribe/>.

144 Amazon Web Services, Amazon Translate, n.d., <https://aws.amazon.com/translate/>.

145 Biesecker et al., ‘As Israel Uses US-Made AI Models in War, Concerns Arise about Tech’s Role in Who Lives and Who Dies’, 18 February 2025.

146 Harry Davies and Yuval Abraham, ‘Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support during Gaza War’, The Guardian (Jerusalem), 23 January 2025, <https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft>.

147 Yuval Abraham, ‘Leaked Documents Expose Deep Ties between Israeli Army and Microsoft’, +972 Magazine, 23 January 2025, <https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/>.

148 Microsoft, What Is the Speech Service?, 5 November 2025, <https://learn.microsoft.com/en-us/azure/ai-services/speech-service/overview>.

149 Microsoft, What Is the Speech Service?

4.3. SPEECH ANALYTICS

While transcription and translation convert raw audio into searchable and analyzable text, the next step in Israel's voice-surveillance infrastructure likely involves the use of speech analytics, which news reporting suggests to include keyword searching and content flagging, sentiment analysis, and pattern recognition.

Keyword searching and flagging

A foundational feature of speech analytics is keyword searching. This enables the identification of relevant content within large amounts of intercepted data. An intelligence officer, speaking to AP News, described using Azure to quickly search for terms in transcripts of “conversations between two people within a 50-page document.”¹⁵⁰ In addition to Azure, +972 Magazine reported that Unit 8200 uses its own smaller models to classify information and conduct “efficient keyword searches” across voice-surveillance data.¹⁵¹

Additionally, AP News also noted that Israeli military uses “to sift through vast troves of intelligence, intercepted communications and surveillance to find suspicious speech or behavior,”¹⁵² though the exact tools used remain unspecified. This type of flagging can be done via a number of different techniques, but most likely involve automatically scanning text transcripts of voice data for pre-determined terms.

This capability has been proven to be used previously for written text messages in a system called “noisy message,” also developed by Unit 8200 after 2015 and still in use today.¹⁵³ This system “collects Palestinians’ text messages and assigns each of them a rating indicating their level of “danger.”¹⁵⁴ Sources told The Guardian that said rating is based on an automated scan of all text messages between Palestinians in the West Bank in search of words deemed to be suspicious.¹⁵⁵

Sentiment analysis

Sentiment analysis enables the identification of emotional states or intent within intercepted conversations. This can be conducted both on the audio itself (by analysing vocal markers such as the volume of a voice or the tightness of vocal cords) and on the transcribed text (via keyword analysis and content assessment). While not confirming which of the two approaches—if not both—is deployed, sources of The Guardian indicate that sentiment models are used to “automatically analyse intercepted phone conversations by identifying Palestinians expressing anger.”¹⁵⁶ These capabilities may be powered by smaller language models developed by Unit 8200, alongside or in addition to Azure’s cloud-based tools, deployed “on-prem,”

150 Biesecker et al., ‘As Israel Uses US-Made AI Models in War, Concerns Arise about Tech’s Role in Who Lives and Who Dies’, 18 February 2025.

151 Abraham, ‘Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians’.

152 Biesecker et al., ‘As Israel Uses US-Made AI Models in War, Concerns Arise about Tech’s Role in Who Lives and Who Dies’, 18 February 2025.

153 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

154 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

155 Davies and Abraham, “‘A Million Calls an Hour’: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

156 Davies and Abraham, ‘Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data’.

short for ‘on premise,’ which means on the unit’s own servers, and in this case in a segregated environment disconnected from the internet.¹⁵⁷

Pattern recognition

There is some indication that Israel uses “a foundational model”¹⁵⁸ that aims to “take ‘everything that has ever been collected’ and detect ‘connections and patterns which are difficult for a human to do alone.’”¹⁵⁹ Further details on this model are not available, but it was reported that Israeli private sector experts contributed to building it during their reserve duty.¹⁶⁰

OpenAI’s language model through Microsoft Azure

It was reported that Israel’s military has access to OpenAI’s GPT-4 model for the purposes of “analyzing billions of pieces of information, learning from past cases, and responding to spoken and written instructions.”¹⁶¹ Documents reviewed by +972 Magazine revealed that the Israeli military consumes substantial AI services from Azure, a quarter of that consumption being for GPT-4.¹⁶² While a spokesperson for the company stated that “OpenAI does not have a partnership with the [Israeli military],”¹⁶³ Microsoft began offering OpenAI’s models as part of its Azure suite of offerings after investing billions of dollars in the company. Indeed, as the +972 Magazine reporting revealed, beginning in August 2023, the Israeli army “acquires access through the Azure platform rather than directly from OpenAI”¹⁶⁴ (emphasis added). The fact that “OpenAI’s commercial services can be accessed only through Azure” exemplifies a broader algorithmic supply chain trend where “AI-specific providers’ services can be accessed only [...] that specific provider’s cloud, rather than through a competitor.”¹⁶⁵

The processes and technologies outlined above enable the large-scale identification, transcription, translation, processing, and analysis of voice data. Once this information is processed, it can be leveraged for a variety of applications.

5. APPLICATIONS FOR VOICE DATA

Publicly available information indicates four primary applications for processed and analyzed voice data: (1) direct reporting to military and intelligence units; (2) integration with other databases through data fusion; (3) use as training material for a large language model; and (4) use as input into an automated target-generation system.

157 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War’.

158 Davies and Abraham, ‘Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data’.

159 Davies and Abraham, ‘Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data’.

160 Davies and Abraham, ‘Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data’.

161 Abraham, ‘Leaked Documents Expose Deep Ties between Israeli Army and Microsoft’.

162 Abraham, ‘Leaked Documents Expose Deep Ties between Israeli Army and Microsoft’.

163 Abraham, ‘Leaked Documents Expose Deep Ties between Israeli Army and Microsoft’.

164 Abraham, ‘Leaked Documents Expose Deep Ties between Israeli Army and Microsoft’.

165 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1191.

5.1. DIRECT REPORTING

A core application of processed voice data is the direct dissemination of translated transcripts to operational units. As reported by Middle East Eye in 2021, transcribed “texts are translated and sent to the army’s intelligence units and to Shin Bet.”¹⁶⁶ More recent reporting corroborates this workflow: commanders “can access raw intelligence translated into Hebrew.”¹⁶⁷ In practice, this means that intercepted voice conversations—once transcribed and translated—provide raw intelligence distributed to Israeli military and internal security agencies.

5.2. DATA FUSION

Public information about how voice-surveillance data is integrated with other data remains limited, but available sources indicate that it forms part of a broader set of databases. Yossi Sarel, former head of Unit 8200 and chief architect of its AI strategy, supposedly “led a large-scale, well-funded project that dramatically expanded Israel’s surveillance of Palestinians and integrated multiple intelligence databases.”¹⁶⁸ While the exact databases with which voice data is integrated are not specified, Sarel’s writings suggest cross-referencing of “visual information, cellular data, social media connections, pictures, cellphone contacts,” and potentially more,¹⁶⁹ echoing Elia Zureik’s characterization of Israel’s layers of mass surveillance data collection.¹⁷⁰

Examples of such data fusion appear in recent reporting. AP News mentioned that information gathered through mass surveillance “can then be cross-checked with Israel’s in-house targeting systems and vice versa.”¹⁷¹ Azure-based tools reportedly “find people giving directions to one another,” which can be cross-referenced with military geolocation systems to pinpoint specific locations.¹⁷² This integration of voice data with geolocation may shed light on an unnamed AI audio tool deployed by the Israeli military in Gaza to locate resistance leaders, giving an approximate location for where they were making phone calls.¹⁷³

166 Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’.

167 Abraham, ‘Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians’.

168 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

169 Harry Davies and Bethan McKernan, ‘Top Israeli Spy Chief Exposes His True Identity in Online Security Lapse’, *The Guardian*, 5 April 2024, <https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse>.

170 Zureik, ‘Colonialism, Surveillance, and Population Control’, 12–13.

171 Biesecker et al., ‘As Israel Uses US-Made AI Models in War, Concerns Arise about Tech’s Role in Who Lives and Who Dies’, 18 February 2025.

172 Biesecker et al., ‘As Israel Uses US-Made AI Models in War, Concerns Arise about Tech’s Role in Who Lives and Who Dies’, 18 February 2025.

173 Sheera Frenkel and Natan Odenheimer, ‘Israel’s A.I. Experiments in Gaza War Raise Ethical Concerns’, *The New York Times*, 25 April 2025, <https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html>.

5.3. TRAINING DATA FOR LARGE LANGUAGE MODEL

Voice-surveillance data is also used as training material for a large language model (LLM) being developed by Unit 8200. An investigation by The Guardian revealed that the unit is building an LLM specifically to inquire about the communications it intercepts from Palestinians. The amount of training data required for such a model demonstrates the unit's "large-scale retention of the content of intercepted communications,"¹⁷⁴ potentially far more than the supposed retention period of about a month.¹⁷⁵ The project of building this LLM is supported by "The Studio," linking Unit 8200 with private-sector experts from companies such as Meta, Google, Microsoft, and other firms,¹⁷⁶ whose assistance was specifically sought by the unit.¹⁷⁷

According to Ori Goshen, co-CEO of Israeli company AI21 Labs which specializes in language models and, too, aided Unit 8200, LLMs are advantageous due to "their ability to retrieve data scattered across multiple sources. Rather than using 'primitive search tools,' officers could simply 'ask questions and get answers' from a chatbot."¹⁷⁸ The conversational chatbot could be queried, for example, about "whether two people had ever met."¹⁷⁹ Reporting suggests that while the development of this LLM began prior to October 2023,¹⁸⁰ it accelerated in late 2024 with additional private sector support. It remains unclear whether the model has already been deployed.¹⁸¹

The rationale for using voice-surveillance data for this LLM as opposed to an existing model is straightforward. Spoken Palestinian Arabic—whether from transcripts of calls or WhatsApp conversations—is scarcely available online, especially "in the quantity needed to train such a model."¹⁸² Existing commercial or open-source Arabic models are trained predominantly on standard written Arabic, not the spoken dialects used by Palestinians on a day-to-day basis. Unit 8200 therefore collected "all the [spoken Arabic] text the unit has ever had" and consolidated it in a central repository to be used as a training dataset.¹⁸³

Sources told The Guardian that this dataset ultimately comprised roughly 100 billion words, covering Palestinian and Lebanese dialects. So even when intercepted conversations had no value for strictly military intelligence purposes, they were still valuable to Unit 8200 for the training and accuracy of their model.

174 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

175 Davies and Abraham, "A Million Calls an Hour": Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians'.

176 The Times of Israel, 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report'.

177 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

178 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

179 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

180 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

181 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

182 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

183 Davies and Abraham, 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'.

A separate chatbot to Unit 8200's LLM was announced by Shin Bet in 2023, and intended to be established on the agency's own servers.¹⁸⁴ However, it is unknown whether this chatbot relied on voice-surveillance data as training data.

5.4. INPUT DATA FOR MILITARY TARGET GENERATION ALGORITHM

Finally, voice data is reportedly used as one input—alongside other data sources—into automated target-generation systems, most prominently the one known as Lavender.¹⁸⁵ Lavender assigns individuals in Gaza a numerical “risk score,” the threshold above which designates them as a human target.¹⁸⁶ But, as Human Rights Watch cautions, without access to Lavender it is impossible to fully determine which data points contribute to these scores.¹⁸⁷

Nevertheless, there are multiple news reports indicating that voice-surveillance data feeds into target-generation algorithms like Lavender. According to +972 Magazine, three intelligence sources stated that Unit 8200's cloud-based intelligence corpus—containing voice data—has been used over the past two years to plan lethal airstrikes in Gaza.¹⁸⁸ The Guardian further exposed that the “enormous repositories of phone calls” stored in Azure were used to identify bombing targets.¹⁸⁹

In line with their writings on the quotidian violence of Israeli surveillance, Shalhoub-Kevorkian and Otman articulate how systems like Lavender “dehumanize and marginalize the surveilled,” reducing human beings to risk assessment scores rather than recognizing their humanity.¹⁹⁰ Through this lens, voice data becomes one more datapoint used to algorithmically classify, rate, and select human targets.¹⁹¹

6. LIMITATIONS OF ALGORITHMIC VOICE TECHNIQUES

Israel's voice-surveillance apparatus combines components—speech-to-text tools, AI-powered translation, voice recognition, and large language models—that are prone to errors and inaccuracies that can lead to the misidentification of people and the misinterpretation of speech. Their technical

184 Yuval Mann and Korin Elbaz-Alush, ‘Shin Bet Develops ChatGPT-like Tool for Detecting Threats, Chief Ronen Bar Says’, YNet, 27 June 2023, <https://www.ynetnews.com/business/article/hjmohud002>.

185 Yuval Abraham, ‘Lavender’: The AI Machine Directing Israel's Bombing Spree in Gaza, 3 April 2024, <https://www.972mag.com/lavender-ai-israeli-army-gaza/>.

186 Human Rights Watch, Questions and Answers: Israeli Military's Use of Digital Tools in Gaza, 10 September 2024, <https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza>.

187 Human Rights Watch, Questions and Answers: Israeli Military's Use of Digital Tools in Gaza.

188 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

189 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

190 Shalhoub-Kevorkian and Otman, ‘Secrecy as Colonial Violence: The Case of Occupied East Jerusalem’, 191.

191 Sarah Fathallah, ‘Artificial Intelligence and the Orchestration of Palestinian Life and Death’, Tech Policy Press, 12 August 2025, <https://www.techpolicy.press/artificial-intelligence-and-the-orchestration-of-palestinian-life-and-death/>.

failures carry real-world consequences, including wrongful arrests and lethal targeting.

AI-driven transcription and translation tools often misinterpret words or context. For example, one reported error in Israel's voice-surveillance system involved the Arabic term for "payment" being mistranslated as a "the grip on the launch tube for a rocket-propelled grenade," nearly placing individuals on target lists erroneously.¹⁹² The chatbot developed by Unit 8200 too "had difficulty identifying modern slang and words transliterated from English."¹⁹³ This is far from an anomaly, as automatic speech recognition in Arabic demonstrates subpar accuracy rates.¹⁹⁴ Dialectal and pronunciation variations introduce additional complications¹⁹⁵ and aggravate misinterpretations, as shown by a case where a Palestinian refugee was incorrectly classified as Syrian based on his pronunciation of a single syllable.¹⁹⁶ These errors persist even when human review is supposedly involved. Arabic-speaking officers may catch some mistakes,¹⁹⁷ but confirmation bias¹⁹⁸ and added work¹⁹⁹ mean errors can go uncorrected, or commanders may want to bypass military language centers and linguistic experts entirely.²⁰⁰

Beyond translation, 'hallucinations'—algorithmic model outputs that are generated without basis in the source material—pose further risks. If in use by Unit 8200, OpenAI's translation model Whisper and other transcription tools are known to fabricate text, including "adding racial commentary and violent rhetoric."²⁰¹ Sources admit that "blind reliance on these tools" is possible,²⁰² raising the risk that decisions are influenced by information that never actually existed.

Furthermore, voiceprinting technologies have high false-positive rates,²⁰³ and sentiment analysis that entails emotion recognition from one's speech

192 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

193 The Times of Israel, 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report'.

194 Fawaz S. Al-Anzi and Dia AbuZeina, 'Synopsis on Arabic Speech Recognition', *Ain Shams Engineering Journal* 13, no. 2 (2022): 101534, <https://doi.org/10.1016/j.jasej.2021.06.020>.

195 Daniel Leix Palumbo and Robert Prey, 'Sounding out Voice Biometrics: Comparing and Contrasting How the State and the Private Sector Determine Identity through Voice', *Big Data & Society* 11, no. 4 (2024): 20539517241297889, <https://doi.org/10.1177/20539517241297889>.

196 Karin Bijsterveld and Anna Kivalova, 'Forensic Voices: Cultures of Sonic Detection and Identification in the West', *Sound Studies* 9, no. 2 (2023): 156, <https://doi.org/10.1080/20551940.2023.2232211>.

197 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

198 Michael Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', *AP News*, 18 February 2025, <https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108>.

199 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

200 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

201 Biesecker et al., 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies', 18 February 2025.

202 Abraham, 'Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians'.

203 Jay Stanley, 'On the Creation of Giant Voiceprint Databases', *ACLU*, 16 October 2014, <https://www.aclu.org/news/privacy-technology/creation-giant-voiceprint-databases>.

is widely decried as unreliable,²⁰⁴ reflecting both the technical limitations and the dangers of misapplied biometric identification and emotion inference.

These limitations are exacerbated by the fact that some of these tools operate as ‘black boxes,’ with limited visibility into how algorithmic systems generate outputs or make recommendations, blocking the possibility of tracing how conclusions are reached or correcting mistakes. However, reducing error rates may not be of concern to Israel at all: Israeli sources stated that “the most pressing issue is not necessarily the accuracy of these models, but rather the vast scope of arrests they enable.” For them, the most important objective was to continuously grow the list of “suspects,”²⁰⁵ regardless of accuracy.

7. IMPACTS ON PALESTINIANS

Israeli voice surveillance has profound effects on Palestinians, shaping daily life through incrimination, criminalization, and deadly consequences. These impacts remain inseparable from the broader militarized and carceral context of the occupation.

Incrimination and arrests

Voice-surveillance data directly facilitates the arrests of Palestinians. The increased scope of surveillance enabled by Unit 8200’s large-scale voice datasets have allowed commanders to compile expansive suspect lists across Palestinian localities, expressly contributing to a greater number of arrests.²⁰⁶ The number and frequency of arrests can be arbitrarily pre-determined, and sometimes, “it’s just a division commander who wants 100 arrests per month in his area,” as one source disclosed.²⁰⁷ The low threshold for suspicion—often vague or unsubstantiated—enables authorities to justify detention, blackmail, or even targeted killings retroactively, using voice data to legitimize their decisions. As one source told *The Guardian*, “[w]hen they need to arrest someone and there isn’t a good enough reason to do so, that’s where they find the excuse,” referring to the voice-surveillance data stored in the cloud.²⁰⁸ The development of Unit 8200’s large language model is predicted to accelerate the incrimination and arrest of Palestinians, worsening existing “figures showing that nearly 50 per cent of adult Palestinians in the occupied territories have been arrested at one time or another.”²⁰⁹

Chilling and criminalization of speech

The pervasive monitoring of Palestinians’ conversations creates a climate of fear and self-censorship.²¹⁰ “Aware that what they say [...] may be observed

204 Jade McClain, ‘Alexa, Am I Happy? How AI Emotion Recognition Falls Short’, New York University, 18 December 2023, <https://www.nyu.edu/about/news-publications/news/2023/december/alexam-i-am-i-happy-how-ai-emotion-recognition-falls-short.html>.

205 Abraham, ‘Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians’.

206 Davies and Abraham, ‘Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data’.

207 Abraham, ‘Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians’.

208 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

209 Zureik, *Israel’s Colonial Project in Palestine*, 163.

210 Zureik, ‘Colonialism, Surveillance, and Population Control’, 16.

constantly,”²¹¹ Palestinians refrain from political expression or avoid speaking as freely as they might want to,²¹² anticipating that their conversations could serve as incriminating or incitement material.²¹³ The sweeping incitement laws put in place by Israel made way for incitement to become a common charge and intimidate Palestinians into silence,²¹⁴ including and especially human rights defenders.²¹⁵

This chilling effect takes on particularly urgent dimensions in contexts where communications can mean access to life-or-death information. As one Gaza hospital administrator explained, the constant awareness of being watched «twisted and narrowed his world» to the point where he «avoids calling his brother lest he ask whether any rockets were fired from the area or whether the Israelis had arrived in the area,’ and those words be misread or distorted by unseen listeners.»²¹⁶ Voice surveillance thus not only chills political expression, but prevents Palestinians from seeking life-saving information about military movements, safety conditions, or humanitarian access.

Killings and assassinations

Voice surveillance can also be directly tied to lethal outcomes. If voice-surveillance data is indeed being used as input in the Israeli military’s automated target-generation systems, those consequences are even more catastrophic.²¹⁷ One tragic example reported by the Los Angeles Times is the case of Jumana, a mother who was killed in an Israeli airstrike along with her 4-day-old twins in Gaza, and whose family and colleagues suspected was wrongly targeted using AI and phone data. A friend of the family said: “There’s just no justification. None,” adding that “[t]he Israelis have all this technology. They target with artificial intelligence, they strike based on voiceprint, on phone signals. Couldn’t they verify? Why did they attack this family?”²¹⁸

Together, incrimination, chilling of speech, and lethal targeting illustrate the grave dangers and consequences of voice surveillance for Palestinians, making it all the more urgent and critical to contest and resist this apparatus.

211 Zureik, ‘Colonialism, Surveillance, and Population Control’, 17.

212 Usaid Siddiqui, “‘Chilling Effect’: Israel’s Ongoing Surveillance of Palestinians”, Al Jazeera, 8 May 2023, <https://www.aljazeera.com/news/2023/5/7/chilling-effect-israels-ongoing-surveillance-of-palestinians>.

213 Sophia Goodfriend, ‘When Palestinian Political Speech Is “Incitement”’, Jewish Currents, 15 September 2021, <https://jewishcurrents.org/when-palestinian-political-speech-is-incitement>.

214 Goodfriend, ‘The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights’, 9.

215 Human Rights Watch, ‘Spyware Used to Hack Palestinian Rights Defenders’.

216 Mhawish, ‘Watched, Tracked, and Targeted’.

217 Sarah Fathallah, ‘Algorithmic Death-World: Artificial Intelligence and the Case of Palestine’, *Public Humanities* 2 (2026): e7, <https://doi.org/10.1017/pub.2025.10113>.

218 Nabih Bulos, ‘He Went to Register the Birth of His Twins. He Returned to Find Them Killed in an Israeli Strike’, Los Angeles Times, 14 August 2024, <https://www.latimes.com/world-nation/story/2024-08-14/four-day-old-twins-israeli-airstrike>.

8. POTENTIAL AVENUES FOR CONTESTATION

Various actors are entangled in the voice surveillance of Palestinians, complicating accountability for its impacts on Palestinians, but also creating multiple potential avenues for contestation. These leverage points also emerge because the voice-surveillance ecosystem can be challenged by a number of actors—employees, investors, foreign governments, civil society organizations, and investigative journalists.

8.1. FRAGMENTED ACCOUNTABILITY

When looking at the voice-surveillance architecture as a whole, many actors appear to operate in concert with one another. Core players in the voice-surveillance supply chain include Israeli military and government units (such as Unit 8200 and Shin Bet), Israeli private tech firms (such as AI21 Labs and NSO), and cloud providers (such as Microsoft and Amazon). Helga Tawil-Souri discusses the importance of understanding relations of power in digital infrastructures, as, in her opinion, tracing “digital surveillance routes” allows one to realize how “Israel would emerge in spaces where it would control, own and manage [those] nodes.”²¹⁹

Data-driven supply chains are supply chains where “the flow of data between actors links them together, [and] where several actors contribute towards the production, deployment, use, and functionality of AI technologies.”²²⁰ What emerges from these orchestrations is what is known by technologists as ‘the problem of the many hands.’²²¹ This problem stems from the fact that no one actor working in isolation is responsible for outcomes that a group of multiple actors contribute towards in different ways. As such, responsibility for these systems is distributed across a complex ecosystem of actors, making it difficult “to pinpoint precisely where responsibility for human rights violations lies,”²²² and thus creating significant fragmenting accountability.

Secrecy and evasion further compound the challenge of fully comprehending the actors and the roles they play in the voice-surveillance supply chain.²²³ Israel’s military units frequently decline to comment on their affairs, while foreign tech companies, including Microsoft, have publicly claimed ignorance of how their platforms were used—even when employees of local subsidiaries indicate otherwise.²²⁴ Additionally, whereas some Israeli firms forming part of this apparatus are known, as is the case for NSO and AI21 Labs, it is quite possible—if not likely—that more companies are involved. For instance, Israeli tech firm Comm-IT supported the Israeli

219 Tawil-Souri, ‘Israel’s Telecommunications Lines and Digital Surveillance Routes’, 208.

220 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1186.

221 Helen Nissenbaum, ‘Accountability in a Computerized Society’, *Science and Engineering Ethics* 2, no. 1 (1996): 25–42, <https://doi.org/10.1007/BF02639315>.

222 Amnesty International, *Algorithmic Accountability Toolkit* (2025), <https://www.amnesty.org/en/latest/research/2025/12/algorithmic-accountability-toolkit/>.

223 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

224 Davies and Abraham, “A Million Calls an Hour”: Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians’.

military with migrating its data into the cloud platforms after Google and Amazon established their data centers in Israel, but it's unclear if its role relates to migrating voice-surveillance data specifically.²²⁵ Other forms of voice surveillance have also been reportedly developed by Israeli private firms, including Toka, a company behind a tool that eavesdrops on drivers through their car's microphone, but it is not clear if it is being deployed on Palestinians.²²⁶ In other words, there are probably other actors in the Israeli private tech sector that could be a part of this voice-surveillance architecture, though not all known to the public.

Nevertheless, even though many actors form part of this data-driven supply chain, it is crucial to recognize that their arrangements are asymmetric. Some actors, especially the Israeli military and cloud service providers, hold more relative systemic importance, while others may complete more peripheral tasks. Unit 8200—and the Israeli military writ large—occupies a central position as the entity that builds in-house voice analysis tools and models, enlists the support of other actors, acquires their technologies, as well as shares or obtains voice data with and from them. But experts also acknowledge that “major cloud providers who often control underlying technologies [hold] important positions across supply chains in many sectors.”²²⁷ Ultimately, these “asymmetries of interdependence produce asymmetries in power,”²²⁸ where major actors are systemically more important in bearing the responsibility for a supply chain's outcomes.²²⁹ Big Tech companies like the direct providers previously mentioned in this report as well as those investing in, acquiring, or otherwise supporting the Israeli firms involved in Israel's voice-surveillance architecture—for example, Nvidia, who is in talks to acquire AI21 Labs²³⁰—have de facto more power in the supply chain. When condemning the life-and-death impact of this voice-surveillance supply chain, it is important to keep in mind who has more relative responsibility and power.

8.2. ACTORS WITH POTENTIAL LEVERAGE

Employees and corporate insiders

Employees within technology companies may hold some degree of influence over whether their employers' technologies are developed, maintained, and sold. Employee-led activism has proven pivotal in Microsoft's case. The worker-led campaign group No Azure for Apartheid organized a series of protests at the company's U.S. headquarters and offices, demanding an end to contracts supporting the Israeli military.²³¹ Employees' knowledge of internal operations also comes into play when whistleblowers and internal sources share insider information to journalists for further public knowledge

225 Abraham, “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel's War’.

226 ‘Israeli Firms Turn Connected Cars into Surveillance Tools – Israeli Media’, The Palestine Chronicle, 18 February 2026, <https://www.palestinechronicle.com/israeli-firms-turn-connected-cars-into-surveillance-tools-haaretz-investigation/>.

227 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1187.

228 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1190.

229 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1192.

230 ‘Nvidia in Advanced Talks to Buy Israel's AI21 Labs for up to \$3 Billion, Report Says’, Reuters, 30 December 2025, <https://www.reuters.com/business/nvidia-advanced-talks-buy-israels-ai21-labs-up-3-billion-report-says-2025-12-30/>.

231 Davies and Abraham, ‘Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians’.

and scrutiny, for instance disclosing how Unit 8200 used Azure services to store voice-surveillance data.²³²

Investors and shareholders

Investors wield financial and governance leverage in the companies whose shares they hold, often through formal proposals or direct engagement with corporate leadership. In July 2025, at least 60 Microsoft investors—collectively representing over \$80 million in shares—filed a proposal requesting a comprehensive assessment of the company’s human rights due diligence processes, “in the face of serious allegations of complicity in genocide and other international crimes.”²³³ Specifically, investors requested that Microsoft assess how its AI and cloud technologies are being misused by military clients “to commit human rights abuses or violations of international humanitarian law,”²³⁴ after investigations revealed the company’s role in storing troves of Palestinian voice-surveillance data.

In December 2025, Norway’s \$2.1 trillion sovereign wealth fund—the world’s largest and a major Microsoft shareholder—announced that it would support a shareholder vote requiring Microsoft to report on human rights risks in countries with significant concerns. Though not explicitly naming Israel, the proposal demanded transparency regarding how Microsoft identifies human rights dangers posed by its products and evaluates whether its internal controls effectively prevent abuses.²³⁵ A few days later at Microsoft’s annual shareholder meeting, these human rights proposals gained significant traction, securing support from more than a quarter of voting shares.²³⁶

Civil society organizations and activists

NGOs, advocacy groups, and grassroots activists provide critical public oversight. Their strategies include campaigns, petitions, protests, and media engagement. For example, an activist group, Geef Tegengas (Push Back), staged demonstrations on the rooftops of Microsoft data centers in the Netherlands, urging employees to withhold their labor and “lay down their work until all Israeli intelligence has been removed from the servers,”²³⁷ in response to news that Unit 8200 was using Azure’s cloud platform, notably the data centers in the Netherlands, to store intercepted Palestinian voice data.

232 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

233 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

234 Layne Mullett, ‘Unprecedented Investor Action Demands Microsoft Answer for Reported Involvement in Gaza Genocide’, American Friends Service Committee, 23 July 2025, <https://afsc.org/newsroom/unprecedented-investor-action-demands-microsoft-answer-reported-involvement-gaza-genocide>.

235 Mike Ludwig, ‘Microsoft Faces Reckoning for Assisting Israel’s Genocide in Gaza’, Truthout, 3 December 2025, <https://truthout.org/articles/microsoft-faces-reckoning-for-assisting-israels-genocide-in-gaza/>.

236 Todd Bishop, ‘Filing: Human Rights Proposals Win More than 25% of Votes at Microsoft Shareholder Meeting’, GeekWire, 9 December 2025, <https://www.geekwire.com/2025/filing-human-rights-proposals-win-more-than-25-of-votes-at-microsoft-shareholder-meeting/>.

237 Harry Davies, ‘Activists in Netherlands Protest on Roof of Microsoft Site Storing Israeli Military Data’, The Guardian, 10 August 2025, <https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data>.

Investigative journalists

Independent investigative journalism plays a significant role in revealing abuses. Microsoft only conducted investigations—the first in May 2025²³⁸ and the second in September of the same year²³⁹—into its relationship with Unit 8200 and the harm it causes to Palestinians after The Guardian, +972 Magazine, and other outlets published reports detailing how Azure was used to store and process Palestinian voice data. Investigative journalism not only triggers corporate responses but also informs the public. In fact, much of the information that this report presents on the voice-surveillance architecture deployed by Israel relies on journalistic exposés.

Foreign governments and international bodies

National governments and international bodies have the potential to apply leverage to actors in the voice-surveillance apparatus through trade policy, sanctions, or legal actions. European states, for example, debated measures to prevent the use of EU data centers for hosting voice-surveillance data, while the UN Special Rapporteur has raised the potential for corporate complicity in international crimes, which could be grounds for investigations and prosecutions by the International Criminal Court and national judiciaries.²⁴⁰

8.3. DEMANDS AND POTENTIAL COURSES OF ACTION

Suspension or cancellation of contracts

Direct demands often involve the suspension or termination of contracts, in this case those that underlie Israel's voice-surveillance architecture. In an “extraordinary decision,” Microsoft ultimately “ceased and disabled a set of services to a unit within the Israel ministry of defense”, including cloud storage and AI services, following combined pressure from employees, investors, and investigative reports.²⁴¹ This decision set a new precedent, as this “termination is the first known case of a US technology company withdrawing services provided to the Israeli military” since October 2023.²⁴² However, for some, this was only the first step of many. On the same day of the announcement, No Azure For Apartheid called for Microsoft to cut all its ties with Israel.²⁴³ And shortly thereafter, a group of human rights groups also demanded more from Microsoft, asking its CEO “[w]hat steps, if any, will [the company] take to suspend its business with the Israeli military and other government bodies where there is evidence indicating that business is contributing to grave human rights abuses and international crimes,”²⁴⁴ demanding further accountability and action.

238 Microsoft, ‘Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza’, Microsoft On the Issues, 15 August 2025, <https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/>.

239 Brad Smith, ‘Update on Ongoing Microsoft Review’, Microsoft On the Issues, 25 September 2025, <https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/>.

240 The Office of the High Commissioner for Human Rights, From Economy of Occupation to Economy of Genocide: Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967, A/HRC/59/23 (2025), <https://www.ohchr.org/en/documents/country-reports/ahrc5923-economy-occupation-economy-genocide-report-special-rapporteur>.

241 Davies and Abraham, ‘Microsoft Blocks Israel’s Use of Its Technology in Mass Surveillance of Palestinians’.

242 Davies and Abraham, ‘Microsoft Blocks Israel’s Use of Its Technology in Mass Surveillance of Palestinians’.

243 No Azure For Apartheid, The First Domino Has Fallen — Microsoft Cuts Some Services to Israeli Unit 8200, 25 September 2025, <https://medium.com/@noazureforapartheid/the-first-domino-has-fallen-microsoft-cuts-some-services-to-israeli-unit-8200-b502d63e8b3b>.

244 Access Now et al., Microsoft Must Come Clean on Its Role in Israel’s War on Gaza, 10 October 2025, <https://www.accessnow.org/press-release/microsoft-must-come-clean-on-its-role-in-israels-war-on-gaza/>.

Legal liability

Even though lawsuits have not yielded much material impact in the past, Zureik made a case for cause lawyering, thanks to “mounting interest in the potential of human rights and transnationalism to affect state policies and mobilise refugee communities.” To him, cause lawyering “has proven effective in publicising mistreatment of marginal groups who have no recourse to redressing their grievances through the apparatuses of the nation-state.”²⁴⁵

Companies hosting voice-surveillance data abroad may be exposed to legal liability under the legal corpus of their corresponding jurisdictions, requiring companies to comply with specific conditions to ensure human rights due diligence and abide by data protection and privacy legal provisions. This point was raised in an internal legal opinion from the Israeli Justice Ministry in 2022, which “noted that both France and Germany required corporations to check for human rights violations in their supply chains by law,” adding that if “it were to be revealed that these corporations are operating in the occupied Palestinian territories, such laws ‘may lead to the issuance of orders to prevent or restrict services.’”²⁴⁶ In relation to the voice-surveillance data stored in Azure’s Netherlands-based data centers, the ministry warned that “the Netherlands was working on similar legislation,” concerned that “a potential lawsuit would be particularly harmful to Israel.”²⁴⁷

The Israeli Justice Ministry’s concerns were not entirely unfounded. Revelations about the Israeli military’s reliance on Netherlands-based data centers to store voice-surveillance data prompted parliamentary inquiries, in response to which the Dutch foreign minister proclaimed: “If there are serious indications of criminal offences in that information, legal proceedings can of course be initiated, and that is then up to the public prosecution service.”²⁴⁸ In Ireland, the Irish Council for Civil Liberties formally asked the Irish Data Protection Commission to investigate Microsoft for the “unlawful processing” of the voice data of Palestinians, constituting “a breach of the EU’s general data protection regulation (GDPR) governing use of personal data.”²⁴⁹

Concerns of facing lawsuits can be alleviated by Israel by keeping voice-surveillance data within its jurisdiction. Given that major cloud providers have established their own data centers in Israel, one source told +971 Magazine that this could lessen the fear of legal action from overseas courts.²⁵⁰ This tactic is common in algorithmic supply chains, as actors use whatever “techno-legal strategy” that enables them to reduce risk, and, in the case of cross-border supply chains, make use of regulatory arbitrage.²⁵¹ Israel can also enlist the collaboration of tech companies, as contracts negotiated with the likes of Google and Amazon stipulate that they send a secret code to Israel to tip it off “when it has disclosed Israeli data to foreign courts or

245 Zureik, *Israel’s Colonial Project in Palestine*, 47.

246 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

247 Abraham, ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’.

248 Davies, ‘Activists in Netherlands Protest on Roof of Microsoft Site Storing Israeli Military Data’.

249 O’Carroll, ‘Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF’.

250 Abraham, ‘“Order from Amazon”: How Tech Giants Are Storing Mass Data for Israel’s War’.

251 Cobbe et al., ‘Understanding Accountability in Algorithmic Supply Chains’, 1194–95.

investigators,” as a way “to sidestep legal orders.”²⁵² This would allow Israel to swiftly move its data, as was the case for the data it held in Azure’s data centers in The Netherlands, mere days following The Guardian investigation,²⁵³ something the Irish Council for Civil Liberties considered akin to hiding “evidence of illegal processing before investigations could commence within the EU.”²⁵⁴

Being implicated in the voice-surveillance supply chain can be in breach not only of foreign domestic laws but also international law. As an international coalition of legal and advocacy rights groups—the Abolitionist Law Center, Avaaz Foundation, European Legal Support Center, SOMO, Center for Constitutional Rights, Ekō, and GLAN (Global Legal Action Network)—warned in a notice of exposure to legal liability sent to Microsoft for its involvement in grave human rights violations, including “Israel’s commission of illegal, extensive, and oppressive surveillance of the Palestinian population,” the company “Microsoft has exposed itself, its leadership, and its individual officers to wide-ranging criminal and civil legal liability, including in domestic courts in the United States and the European Union, and before various international bodies”²⁵⁵ such as the International Criminal Court.

Countries that recognize the International Court of Justice’s power may legally challenge companies operating in their jurisdictions if the court ultimately rules the military campaign to be a genocide.²⁵⁶ International humanitarian and human rights law offers avenues for contestation, including litigation in international tribunals and transnational lawsuits, on the grounds of violating key rights as the right to privacy, freedom of expression, and access to the internet.²⁵⁷ Under the Oslo Accords, violating Palestinian sovereignty over ICT infrastructure could also be argued.²⁵⁸

Sanctions and export controls

Governments could impose targeted sanctions, export controls, or blacklisting of companies enabling human rights violations like the ones resulting from Israel’s voice-surveillance apparatus. One example is the U.S. government’s blacklisting of spyware companies NSO Group and Candiru.²⁵⁹ Governments could also impose export controls. However, this is complicated by the “dual-use” nature of technologies used in voice surveillance, which can be used for both military and non-military purposes. For instance, “U.S. export controls were originally created to regulate items with clear military inputs and use cases,” but dual-use technologies that also carry commercial

252 Harry Davies and Yuval Abraham, ‘Revealed: Israel Demanded Google and Amazon Use Secret “Wink” to Sidestep Legal Orders’, The Guardian, 29 October 2025, <https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code>.

253 Davies and Abraham, ‘Microsoft Blocks Israel’s Use of Its Technology in Mass Surveillance of Palestinians’.

254 O’Carroll, ‘Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF’.

255 Abolitionist Law Center, ‘Microsoft’s Aiding of Israel’s Genocide Against Palestinians Exposes Company and Its Leadership to Legal Liability’, Abolitionist Law Center, 2 December 2025.

256 Ryan Grim and Waqas Ahmed, ‘The Israeli Military Is One of Microsoft’s Top AI Customers, Leaked Documents Reveal’, Drop Site, 23 January 2025, <https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud>.

257 Anan AbuShanab, Connection Interrupted: Israel’s Control of the Palestinian ICT Infrastructure and Its Impact on Digital Rights (7amleh – The Arab Center for the Advancement of Social Media, 2018), 27, https://7amleh.org/wp-content/uploads/2019/01/Report_7amleh_English_final.pdf.

258 Abdullah and Bahour, ICT: The Shackled Engine of Palestine’s Development.

259 Masarwa, ‘Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source’.

applications “are more difficult to regulate at both the national and international levels.”²⁶⁰

The fragmented accountability and asymmetrical power dynamics of Israel’s voice-surveillance ecosystem’s create multiple leverage points for challenging its operations, from employee activism and investor pressure to legal action and international scrutiny. While Microsoft’s precedent-setting termination of services to Israeli military units demonstrates the effectiveness of coordinated contestation, demands for further accountability and more decisive action highlight that this remains only one step in a broader struggle. Ultimately, the contested nature of this surveillance architecture—revealed through investigative journalism and scrutinized through regulatory, legal, and public pressure—offers pathways to disrupt the systems enabling Israel’s algorithmic voice surveillance of Palestinians.

CONCLUSION

‘Captive Voices’ speaks to the profound violation at the heart of Israel’s mass algorithmic voice surveillance: the systematic capture of Palestinian speech as a mechanism for their oppression. The preceding chapters have shown that the voice-surveillance apparatus deployed over Palestinians is not a discrete or isolated program, but a dense, multilayered system of capture, storage, analysis, and operational use. What emerges is an architecture of control in which voice data—an intimate, ephemeral trace of everyday life—is embedded in a broader project of population control, connected to other modes of Israeli mass surveillance. This voice-surveillance architecture deeply impacts Palestinian life: constraining communication, producing fear, and facilitating incrimination, arrests, and death.

Even within this architecture of digital control, pathways for contestation emerge. The systematic voice surveillance of Palestinians reveals not only the scale of Israel’s military occupation but also the pivotal role of corporations, technology companies, and cloud service providers, all of whom can be pressured through various means. Cases like Microsoft show that actors in this apparatus are not immovable: under sustained pressure from workers, investors, journalists, civil society, and governments, they can be compelled to suspend contracts, adjust practices, or confront their own complicity in human rights abuses.

Yet, contesting this voice-surveillance apparatus means also confronting the carceral and colonial logics that made such a system imaginable and implementable in the first place. Without addressing these underlying structures—including the normalization of mass surveillance and data collection, the legal exceptionalism applied to Palestinians, and the global diplomatic and market incentives that reward Israel’s securitization industry—efforts at reform risk reproducing the very logics they seek to undo.

260 Hannah Kelley, ‘Dual-Use Technology and U.S. Export Controls’, CNAS Technology Policy Lab, 15 June 2023, <https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls>.

The account presented here is perhaps only the tip of the iceberg of a larger and more opaque voice-surveillance regime, but it provides an initial mapping of how the voice data of Palestinians is intercepted, processed, and weaponized. Ultimately, this report serves as both a documentation and an invitation: a call for further research, broader scrutiny, and coordinated action—all interventions that must remain grounded in the broader struggle for Palestinian human rights, dignity, and self-determination.

REFERENCES

- 7amleh. Aṣ-Ṣabāb al-Filīsīniyyīn Wa-Lmuṣārka Ās-Syāsiya ʿAbra Ṣabakāt at-Ttawāʿul ā-Li-jtimāʿī [Palestinian Youth and Political Participation via Social Media Networks]. 7amleh – The Arab Center for the Advancement of Social Media, 2019. <https://7amleh.org/wp-content/uploads/2019/10/-استطلاع-حملة-1.pdf>.
- 7amleh. Facial Recognition Technology and Palestinian Digital Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2020. <https://7amleh.org/post/facial-recognition-technology-and-palestinian-digital-rights>.
- 7amleh. Gaza Telecommunications Infrastructure: Assessment to Damages and Humanitarian Impact. 7amleh – The Arab Center for the Advancement of Social Media, 2024. <https://7amleh.org/post/impact-of-war-on-gaza-s-telecommunications-infrastructure-en>.
- 7amleh. Intensification of Surveillance in East Jerusalem Since October 2023. 7amleh – The Arab Center for the Advancement of Social Media, 2024. <https://7amleh.org/post/surveillance-and-digital-rights-violations-in-east-jerusalem-en>.
- 7amleh. Netanyahu Imposes Dangerous “Big Brother” Surveillance under the Pretext of a Security Response to the Coronavirus. 23 March 2020. <https://www.apc.org/en/news/7amleh-netanyahu-imposes-dangerous-big-brother-surveillance-under-pretext-security-response>.
- Abdullah, Wassim F., and Sam Bahour. ICT: The Shackled Engine of Palestine’s Development. Al-Shabaka, 2015. https://al-shabaka.org/briefs/ict-the-shackled-engine-of-palestines-development/?generate_pdf=view.
- Abolitionist Law Center. ‘Microsoft’s Aiding of Israel’s Genocide Against Palestinians Exposes Company and Its Leadership to Legal Liability’. Abolitionist Law Center, 2 December 2025.
- Abraham, Yuval. ‘Israel Developing ChatGPT-like Tool That Weaponizes Surveillance of Palestinians’. +972 Magazine, 6 March 2025. <https://www.972mag.com/israeli-intelligence-chatgpt-8200-surveillance-ai/>.
- Abraham, Yuval. ‘Lavender’: The AI Machine Directing Israel’s Bombing Spree in Gaza. 3 April 2024. <https://www.972mag.com/lavender-ai-israeli-army-gaza/>.
- Abraham, Yuval. ‘Leaked Documents Expose Deep Ties between Israeli Army and Microsoft’. +972 Magazine, 23 January 2025. <https://www.972mag.com/microsoft-azure-openai-israeli-army-cloud/>.
- Abraham, Yuval. ‘Microsoft Storing Israeli Intelligence Trove Used to Attack Palestinians’. +972 Magazine, 6 August 2025. <https://www.972mag.com/microsoft-8200-intelligence-surveillance-cloud-azure/>.
- Abraham, Yuval. “‘Order from Amazon’: How Tech Giants Are Storing Mass Data for Israel’s War”. +972 Magazine, 4 August 2024. <https://www.972mag.com/cloud-israeli-army-gaza-amazon-google-microsoft/>.
- AbuShanab, Anan. Connection Interrupted: Israel’s Control of the Palestinian ICT Infrastructure and Its Impact on Digital Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2018. https://7amleh.org/wp-content/uploads/2019/01/Report_7amleh_English_final.pdf.
- Access Now, Amnesty International, Electronic Frontier Foundation, Human Rights Watch, 7amleh, and Fight for the Future. Microsoft Must Come Clean on Its Role in Israel’s War on Gaza. 10 October 2025. <https://www.accessnow.org/press-release/microsoft-must-come-clean-on-its-role-in-israels-war-on-gaza/>.
- Al Jazeera. ‘Al-Duwairi: Al-Āṭilāl Yastadīm Baḥmat al-Ḍūt Wālīn Litqwb Muqātīlī al-Muqāwama Biḥaza بغزة: الدويري: الاحتلال يستخدم بصمة الصوت والعين لتعقب مقاتلي المقاومة بـحزة’. Al Jazeera, 15 April 2025. <https://www.aljazeera.net/news/2025/4/15/الدويري-يستخدم-بصمة-الصوت-الاحتلال>.

- Al Jazeera. 'US Court Bars Israeli Spyware Firm from Targeting WhatsApp Users'. Al Jazeera, 18 October 2025. <https://www.aljazeera.com/news/2025/10/18/us-court-bars-israeli-spyware-firm-from-targeting-whatsapp-users>.
- Al Jazeera. 'What Is Project Nimbus, and Why Are Google Workers Protesting Israel Deal?' Al Jazeera, 23 April 2024. <https://www.aljazeera.com/news/2024/4/23/what-is-project-nimbus-and-why-are-google-workers-protesting-israel-deal>.
- Al-Anzi, Fawaz S., and Dia AbuZeina. 'Synopsis on Arabic Speech Recognition'. Ain Shams Engineering Journal 13, no. 2 (2022): 101534. <https://doi.org/10.1016/j.asej.2021.06.020>.
- Ali, Rabia. 'Is WhatsApp Putting Palestinians at Risk of Being Killed in Gaza?' Anadolu, 30 April 2024. <https://www.aa.com.tr/en/artificial-intelligence/is-whatsapp-putting-palestinians-at-risk-of-being-killed-in-gaza/3206563>.
- Al-Jaafari, Wajdi. "Mas  l  n: jamy' was  il al'itti  l fi falas  in mur  qaba" مس  ولون: جميع وسائل الاتصال في فلسطين مراقبة [Officials: All means of communication in Palestine are monitored]'. Ma'an News Agency, 20 December 2014. <https://www.maannews.net/news/748592.html>.
- Alshurafa, Mohammed. The Impact of the Gaza Blockade and the Destruction of Telecommunications Infrastructure on the Digital Economy Amidst Genocide. 7amleh – The Arab Center for the Advancement of Social Media, 2025. <https://7amleh.org/post/gaza-digital-economy-collapse-en>.
- Amazon Web Services. Amazon Translate. n.d. <https://aws.amazon.com/translate/>.
- Amazon Web Services. Speech to Text Service - Amazon Transcribe. n.d. <https://aws.amazon.com/pm/transcribe/>.
- Amnesty International. Algorithmic Accountability Toolkit. 2025. <https://www.amnesty.org/en/latest/research/2025/12/algorithmic-accountability-toolkit/>.
- Amnesty International. Amnesty International and More than 170 Organisations Call for a Ban on Biometric Surveillance. 7 June 2021. <https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/>.
- Amnesty International. Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware. 8 November 2021. <https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/>.
- AVG. Malware Is Still Spying on You Even When Your Mobile Is Off. 14 September 2018. <https://www.avg.com/en/signal/android-spyware-that-works-when-your-phone-is-off>.
- Barghuthy, Eyad, and Alison Carmel. Silenced Networks: The Chilling Effect among Palestinian Youth in Social Media. 7amleh – The Arab Center for the Advancement of Social Media, 2019. <https://7amleh.org/post/silenced-net-the-chilling-effect-among-palestinian-youth-in-social-media>.
- Batniji, Rajaie. 'Searching for Dignity'. The Lancet 380, no. 9840 (2012): 466–67. [https://doi.org/10.1016/S0140-6736\(12\)61280-X](https://doi.org/10.1016/S0140-6736(12)61280-X).
- Biesecker, Michael, Sam Mednick, and Garance Burke. 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies'. AP News, 18 February 2025. <https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108>.
- Biesecker, Michael, Sam Mednick, and Garance Burke. 'As Israel Uses US-Made AI Models in War, Concerns Arise about Tech's Role in Who Lives and Who Dies'. AP News (Tel Aviv), 18 February 2025. <https://apnews.com/article/israel-palestinians-ai-technology-737bc17af7b03e98c29cec4e15d0f108>.

- Biggar, Paul. Meta and Lavender. 16 April 2024. <https://blog.paulbiggar.com/meta-and-lavender/>.
- Bijsterveld, Karin, and Anna Kvalova. 'Forensic Voices: Cultures of Sonic Detection and Identification in the West'. *Sound Studies* 9, no. 2 (2023): 155–65. <https://doi.org/10.1080/20551940.2023.2232211>.
- Bishop, Todd. 'Filing: Human Rights Proposals Win More than 25% of Votes at Microsoft Shareholder Meeting'. *GeekWire*, 9 December 2025. <https://www.geekwire.com/2025/filing-human-rights-proposals-win-more-than-25-of-votes-at-microsoft-shareholder-meeting/>.
- Breaking the Silence. Military Rule: Testimonies of Soldiers from the Civil Administration, Gaza DCL and COGAT. *Breaking the Silence*, 2022. https://www.breakingthesilence.org.il/inside/wp-content/uploads/2022/07/Military_rule_testimony_booklet.pdf.
- Bulos, Nabih. 'He Went to Register the Birth of His Twins. He Returned to Find Them Killed in an Israeli Strike'. *Los Angeles Times*, 14 August 2024. <https://www.latimes.com/world-nation/story/2024-08-14/four-day-old-twins-israeli-airstrike>.
- Cobbe, Jennifer, Michael Veale, and Jatinder Singh. 'Understanding Accountability in Algorithmic Supply Chains'. 2023 ACM Conference on Fairness Accountability and Transparency, 12 June 2023, 1186–97. <https://doi.org/10.1145/3593013.3594073>.
- Conley, Julia. 'Report Indicates Israel Uses WhatsApp Data in Targeted Killings of Palestinians'. *Truthout*, 19 May 2024. <https://truthout.org/articles/report-indicates-israel-uses-whatsapp-data-in-targeted-killings-of-palestinians/>.
- Davies, Harry. 'Activists in Netherlands Protest on Roof of Microsoft Site Storing Israeli Military Data'. *The Guardian*, 10 August 2025. <https://www.theguardian.com/world/2025/aug/10/activists-in-netherlands-protest-on-roof-of-microsoft-site-storing-israeli-military-data>.
- Davies, Harry, and Yuval Abraham. "'A Million Calls an Hour': Israel Relying on Microsoft Cloud for Expansive Surveillance of Palestinians". *The Guardian*, 6 August 2025. <https://www.theguardian.com/world/2025/aug/06/microsoft-israeli-military-palestinian-phone-calls-cloud>.
- Davies, Harry, and Yuval Abraham. 'Microsoft Blocks Israel's Use of Its Technology in Mass Surveillance of Palestinians'. *The Guardian*, 25 September 2025. <https://www.theguardian.com/world/2025/sep/25/microsoft-blocks-israels-use-of-its-technology-in-mass-surveillance-of-palestinians>.
- Davies, Harry, and Yuval Abraham. 'Revealed: Israel Demanded Google and Amazon Use Secret "Wink" to Sidestep Legal Orders'. *The Guardian*, 29 October 2025. <https://www.theguardian.com/us-news/2025/oct/29/google-amazon-israel-contract-secret-code>.
- Davies, Harry, and Yuval Abraham. 'Revealed: Israeli Military Creating ChatGPT-like Tool Using Vast Collection of Palestinian Surveillance Data'. *The Guardian* (Jerusalem), 6 March 2025. <https://www.theguardian.com/world/2025/mar/06/israel-military-ai-surveillance>.
- Davies, Harry, and Yuval Abraham. 'Revealed: Microsoft Deepened Ties with Israeli Military to Provide Tech Support during Gaza War'. *The Guardian* (Jerusalem), 23 January 2025. <https://www.theguardian.com/world/2025/jan/23/israeli-military-gaza-war-microsoft>.
- Davies, Harry, and Bethan McKernan. 'Top Israeli Spy Chief Exposes His True Identity in Online Security Lapse'. *The Guardian*, 5 April 2024. <https://www.theguardian.com/world/2024/apr/05/top-israeli-spy-chief-exposes-his-true-identity-in-online-security-lapse>.
- De Luce, Dan. 'Wigs, Robotic Guns and Exploding Pagers: Israel Has a Long History of Hunting down Its Enemies'. *NBC News*, 20 September 2024. <https://www.nbcnews.com/investigations/israel-long-history-targeted-killings-enemies-rcna171888>.
- Decoster, Xavier Stephane, Ilhab Jebari, Anat Lewin, and Carlo Maria Rossotto. *The Telecommunication Sector in the Palestinian Territories: A Missed Opportunity for Economic Development*. No. 104263. World Bank Group, 2016. <http://documents.worldbank.org/curated/en/993031473856114803>.
- Demopoulos, Alaina. 'Honk Honk! Can Noise Cameras Reduce "Potential-Fatal" Sound Pollution?' *The Guardian* (New York), 4 October 2023. <https://www.theguardian.com/us-news/2023/oct/04/new-york-noise-cameras>.

- Electronic Frontier Foundation. 'Gunshot Detection'. Street Level Surveillance, n.d. <https://sls.eff.org/technologies/gunshot-detection>.
- Euro-Med Human Rights Monitor. Israeli Telecom Companies Must Adhere to UN Principles, Stop Fully Cooperating with Security Agencies. 13 November 2022. <https://euromedmonitor.org/en/article/5437/Israeli-telecom-companies-must-adhere-to-UN-principles-stop-fully-cooperating-with-security-agencies>.
- Fathallah, Sarah. 'Algorithmic Death-World: Artificial Intelligence and the Case of Palestine'. Public Humanities 2 (2026): e7. <https://doi.org/10.1017/pub.2025.10113>.
- Fathallah, Sarah. 'Artificial Intelligence and the Orchestration of Palestinian Life and Death'. Tech Policy Press, 12 August 2025. <https://www.techpolicy.press/artificial-intelligence-and-the-orchestration-of-palestinian-life-and-death/>.
- Fathallah, Sarah, and Nick Mitchell. 'Occupied Assets: Israeli Neoliberalism and the Datafication of Palestinian Life'. Disjunctions Magazine, January 2026. <https://disjunctionsmag.com/articles/occupied-assets/>.
- Fayyad, Usama, Gregory Piatetsky-Shapiro, and Padhraic Smyth. 'From Data Mining to Knowledge Discovery in Databases'. AI Magazine, 15 March 1996.
- Flensburg, Sofie, and Signe Sophus Lai. 'Follow the Data! A Strategy for Tracing Infrastructural Power'. Media and Communication 11, no. 2 (2023). <https://doi.org/10.17645/mac.v11i2.6464>.
- Frenkel, Sheera, and Natan Odenheimer. 'Israel's A.I. Experiments in Gaza War Raise Ethical Concerns'. The New York Times, 25 April 2025. <https://www.nytimes.com/2025/04/25/technology/israel-gaza-ai.html>.
- Front Line Defenders. OPT/Israel: Six Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware. Front Line Defenders, 2021. <https://www.frontlinedefenders.org/en/statement-report/six-palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware>.
- Goodfriend, Sophia. The Expansion of Digital Surveillance in Jerusalem and Impact on Palestinians Rights. 7amleh – The Arab Center for the Advancement of Social Media, 2021. https://7amleh.org/storage/Digital%20Surveillance%20Jerusalem_7.11.pdf.
- Goodfriend, Sophia. 'When Palestinian Political Speech Is "Incitement"'. Jewish Currents, 15 September 2021. <https://jewishcurrents.org/when-palestinian-political-speech-is-incitement>.
- Grim, Ryan, and Waqas Ahmed. 'The Israeli Military Is One of Microsoft's Top AI Customers, Leaked Documents Reveal'. Drop Site, 23 January 2025. <https://www.dropsitenews.com/p/microsoft-azure-israel-top-customer-ai-cloud>.
- Halabi, Usama. 'Legal Analysis and Critique of Some Surveillance Methods Used by Israel'. In Surveillance and Control in Israel/Palestine: Population, Territory, and Power, edited by Elia Zureik, David Lyon, and Yasmeen Abu-Laban. Routledge Studies in Middle Eastern Politics 33. Routledge, 2011. <https://doi.org/10.4324/9780203845967>.
- Hassan, Zaha, and H. A. Hellyer. Suppressing Dissent: Shrinking Civic Space, Transnational Repression and Palestine-Israel. Oneworld Academic, 2024.
- Human Rights Watch. Questions and Answers: Israeli Military's Use of Digital Tools in Gaza. 10 September 2024. <https://www.hrw.org/news/2024/09/10/questions-and-answers-israeli-militarys-use-digital-tools-gaza>.
- Human Rights Watch. Spyware Used to Hack Palestinian Rights Defenders. 8 November 2021. <https://www.hrw.org/news/2021/11/08/spyware-used-hack-palestinian-rights-defenders>.
- IMEU. Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement. Institute for Middle East Understanding, 2021.
- Investigate. 'Amazon.Com Inc.' The American Friends Service Committee, 7 August 2024. <https://investigate.info/company/amazon>.

- Investigate. 'Microsoft Corp.' The American Friends Service Committee, 29 January 2025. <https://investigate.info/company/microsoft>.
- James, Robin. 'Acousmatic Surveillance and Big Data'. Sounding Out!, 20 October 2014. <https://soundstudiesblog.com/2014/10/20/the-acousmatic-era-of-surveillance/>.
- Jamil, Yassin. "Tafāṭīl Muḥīla ʿan ʾUruq Wa ʾasālib al-Murāqaba as-Sirrya al-Is-rāʾīliya Lil-Hawāṭif al-Jawwāla Lil-Muqāwama al-Filsṭīniya Wal-Lubnāniya" تفاصيل مذهلة عن طرق وأساليب المراقبة السرية الإسرائيلية للهواتف الجوالة للمقاومة الفلسطينية واللبنانية [Shocking Details Emerge about Israel's Covert Methods and Techniques for Monitoring the Mobile Phones of the Palestinian and Lebanese Resistance]. Rai Alyoum, 21 June 2016. <https://www.raialyoum.com/ا-تفاصيل-مذهلة-عن-طرق-وأساليب-المراقبة-ل>.
- Kelley, Hannah. 'Dual-Use Technology and U.S. Export Controls'. CNAS Technology Policy Lab, 15 June 2023. <https://www.cnas.org/publications/reports/dual-use-technology-and-u-s-export-controls>.
- Leix Palumbo, Daniel, and Robert Prey. 'Sounding out Voice Biometrics: Comparing and Contrasting How the State and the Private Sector Determine Identity through Voice'. Big Data & Society 11, no. 4 (2024): 20539517241297889. <https://doi.org/10.1177/20539517241297889>.
- Leufer, Daniel. 'Sonic Surveillance: Why You Don't Want AI Snooping on You'. Access Now, 23 September 2025. <https://www.accessnow.org/ai-snooping/>.
- Ludwig, Mike. 'Microsoft Faces Reckoning for Assisting Israel's Genocide in Gaza'. Truthout, 3 December 2025. <https://truthout.org/articles/microsoft-faces-reckoning-for-assisting-israels-genocide-in-gaza/>.
- Mahmoud, Khalid Walid. 'Voiceprint: From a Verification Tool to a Tracking Technology'. The Peninsula, 19 January 2025. <https://thepeninsulaqatar.com/opinion/19/01/2025/voiceprint-from-a-verification-tool-to-a-tracking-technology>.
- Mann, Yuval, and Korin Elbaz-Alush. 'Shin Bet Develops ChatGPT-like Tool for Detecting Threats, Chief Ronen Bar Says'. YNet, 27 June 2023. <https://www.ynetnews.com/business/article/hjmohud002>.
- Marciano, Avi. 'Israel's Mass Surveillance during COVID-19: A Missed Opportunity'. Surveillance & Society 19, no. 1 (2021): 85–88. <https://doi.org/10.24908/ss.v19i1.14543>.
- Masarwa, Lubna. 'Israel Can Monitor Every Telephone Call in West Bank and Gaza, Says Intelligence Source'. Middle East Eye (Jerusalem), 15 November 2021. <https://www.middleeasteye.net/news/israel-can-monitor-every-telephone-call-west-bank-and-gaza-intelligence-source>.
- McClain, Jade. 'Alexa, Am I Happy? How AI Emotion Recognition Falls Short'. New York University, 18 December 2023. <https://www.nyu.edu/about/news-publications/news/2023/december/alexa--am-i-happy--how-ai-emotion-recognition-falls-short.html>.
- Mhawish, Mohammed R. 'Watched, Tracked, and Targeted'. New York Magazine, 3 December 2025. <https://nymag.com/intelligencer/article/watched-tracked-targeted-israel-surveillance-gaza.html>.
- Microsoft. 'Microsoft Statement on the Issues Relating to Technology Services in Israel and Gaza'. Microsoft On the Issues, 15 August 2025. <https://blogs.microsoft.com/on-the-issues/2025/05/15/statement-technology-israel-gaza/>.
- Microsoft. Microsoft to Launch New Cloud Data Center Region in Israel. 22 January 2020. <https://news.microsoft.com/source/emea/features/microsoft-to-launch-new-cloud-datacenter-region-in-israel/>.
- Microsoft. What Is the Speech Service? 5 November 2025. <https://learn.microsoft.com/en-us/azure/ai-services/speech-service/overview>.
- Mitnick, Josh. 'Here's How the Israeli Army Is Embracing Digital Transformation'. CIO, 8 February 2020.

- Mossad, Marco. 'Are Global Tech Giants Facilitating Israel's War on Gaza?' Al Majalla, 31 May 2024. <https://en.majalla.com/node/318176/science-technology/are-global-tech-giants-facilitating-israel%E2%80%99s-war-gaza>.
- Mossad, Marco. 'Voiceprint Technology: A Commercial Hit with Military Utility'. Al Majalla, 7 February 2024. <https://en.majalla.com/node/310146/science-technology/voiceprint-technology-commercial-hit-military-utility>.
- Mullett, Layne. 'Unprecedented Investor Action Demands Microsoft Answer for Reported Involvement in Gaza Genocide'. American Friends Service Committee, 23 July 2025. <https://afsc.org/newsroom/unprecedented-investor-action-demands-microsoft-answer-reported-involvement-gaza-genocide>.
- Niang, Sophie Marie. 'In Defence of What's There: Notes on Scavenging as Methodology'. Feminist Review 136, no. 1 (2024): 52–66. <https://doi.org/10.1177/01417789231222606>.
- Nissenbaum, Helen. 'Accountability in a Computerized Society'. Science and Engineering Ethics 2, no. 1 (1996): 25–42. <https://doi.org/10.1007/BF02639315>.
- No Azure For Apartheid. The First Domino Has Fallen — Microsoft Cuts Some Services to Israeli Unit 8200. 25 September 2025. <https://medium.com/@noazureforapartheid/the-first-domino-has-fallen-microsoft-cuts-some-services-to-israeli-unit-8200-b502d63e8b3b>.
- O'Brien, Danny, and Jillian C. York. 'A Slow Boat to Fast Data: Why Is Palestine Still Waiting for 3G?' Electronic Frontier Foundation, 11 November 2015. <https://www.eff.org/deeplinks/2015/11/palestine-3g>.
- O'Carroll, Lisa. 'Irish Authorities Asked to Investigate Microsoft over Alleged Unlawful Data Processing by IDF'. The Guardian, 4 December 2025. <https://www.theguardian.com/technology/2025/dec/04/irish-authorities-asked-to-investigate-microsoft-over-alleged-unlawful-data-processing-by-idf>.
- Oslo Accords. Annex III, Concerning Civil Affairs, Israeli Palestinian Interim Agreement on The West Bank and the Gaza Strip (Oslo II). 1995. https://www.peaceagreements.org/media/documents/ag985_56017411a3c68.pdf.
- Palestine Today. "Kayfa tatana Dat almuḥarrarāt al'isrā'īliya al jawwālik šaṣy!?" كيف تتنصت المخابرات الإسرائيلية على جوالك الشخصي؟ [How does Israeli intelligence eavesdrop on your personal mobile phone?]. Palestine Today, 30 December 2013. <https://palestodaytv.com/post/466/كيف-تتنصت-المخابرات-الإسرائيلية-على-جوالك-الشخصي>.
- Privacy International. The Global Surveillance Industry. 2016. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf.
- Reuters. 'Israeli Defense Ministry Launches COVID-19 Voice-Test Study'. Reuters (Jerusalem), 24 March 2020. <https://www.reuters.com/article/world/israeli-defense-ministry-launches-covid-19-voice-test-study-idUSKBN21B2YU/>.
- Reuters. 'Nvidia in Advanced Talks to Buy Israel's AI21 Labs for up to \$3 Billion, Report Says'. 30 December 2025. <https://www.reuters.com/business/nvidia-advanced-talks-buy-israels-ai21-labs-up-3-billion-report-says-2025-12-30/>.
- Sada Social. Sada Social Calls for Immediate Investigation into Meta's Leak of WhatsApp Users' Data to the Israeli Military. 18 May 2024. <https://sada.social/post/sd-soshalydaao-l-thkyk-aaagl-ofory-ltsryb-myta-byanat-mstkhdm-y-oatsab-l-algysh-alsrayly>.
- Sa'di, Ahmad H. Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority. Manchester International Relations. Manchester University Press, 2016.
- Salah, Hana. "Albaḥma as-ḥaūtya" Adāt Isrā'īl Litanfī Syāsat "Attaḥafya al-Jasadya" "البصمة الصوتية" أداة إسرائيل لتنفيذ سياسة "التصفية الجسدية" ["Voiceprints": Israel's Tool for Implementing "Elimination"]. Al-Monitor, 4 February 2014. <https://www.al-monitor.com/ar/contents/articles/originals/2014/02/gaza-israel-islamic-jihad-hamas-mobile-war.html>.

- Salah, Mohamad Ateyyah, Mohamad Shalodi, and Mahmoud Skafi. 'Voiceprint Authentication System'. Palestine Polytechnic University, 2021. <https://scholar.ppu.edu/bitstream/handle/123456789/7547/Voiceprint-Authentication-System.pdf>.
- Shalhoub-Kevorkian, Nadera. *Security Theology, Surveillance and the Politics of Fear*. 1st edn. Cambridge University Press, 2015. <https://doi.org/10.1017/CBO9781316159927>.
- Shalhoub-Kevorkian, Nadera, and Abeer Otman. 'Secrecy as Colonial Violence: The Case of Occupied East Jerusalem'. In *Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik*, edited by Ahmad H. Sa'di and Nur Masalha. I.B. Tauris, 2023. *Secrecy as Colonial Violence*.
- Siddiqui, Usaid. "'Chilling Effect": Israel's Ongoing Surveillance of Palestinians'. Al Jazeera, 8 May 2023. <https://www.aljazeera.com/news/2023/5/7/chilling-effect-israels-ongoing-surveillance-of-palestinians>.
- Smalley, Suzanne. 'NSO Seeks to Overturn WhatsApp Case, Saying It Is "Catastrophic" for the Spyware Maker'. The Record, 20 November 2025. <https://therecord.media/nso-seeks-to-overturn-whatsapp-case>.
- Smith, Brad. 'Update on Ongoing Microsoft Review'. Microsoft On the Issues, 25 September 2025. <https://blogs.microsoft.com/on-the-issues/2025/09/25/update-on-ongoing-microsoft-review/>.
- Stanley, Jay. 'On the Creation of Giant Voiceprint Databases'. ACLU, 16 October 2014. <https://www.aclu.org/news/privacy-technology/creation-giant-voiceprint-databases>.
- Swinhoe, Dan. AWS Launches Israeli Cloud Region in Tel Aviv. 2 August 2023.
- Tawil-Souri, Helga. 'Digital Occupation: Gaza's High-Tech Enclosure'. *Journal of Palestine Studies* 41, no. 2 (2012): 27–43. <https://doi.org/10.1525/jps.2012.XLI.2.27>.
- Tawil-Souri, Helga. 'Hacking Palestine: A Digital Occupation'. Al Jazeera, 9 November 2011. <https://www.aljazeera.com/opinions/2011/11/9/hacking-palestine-a-digital-occupation>.
- Tawil-Souri, Helga. 'Israel's Telecommunications Lines and Digital Surveillance Routes'. In *Decolonizing the Study of Palestine: Indigenous Perspectives and Settler Colonialism after Elia Zureik*, edited by Ahmad H. Sa'di and Nur Masalha. I.B. Tauris, 2023.
- Tawil-Souri, Helga. 'Surveillance Sublime: The Security State in Jerusalem'. *Jerusalem Quarterly*, no. 68 (December 2016): 56–65. <https://doi.org/10.70190/jq.l68.p56>.
- The Office of the High Commissioner for Human Rights. *From Economy of Occupation to Economy of Genocide: Report of the Special Rapporteur on the Situation of Human Rights in the Palestinian Territories Occupied since 1967*. A/HRC/59/23. 2025. <https://www.ohchr.org/en/documents/country-reports/ahrc5923-economy-occupation-economy-genocide-report-special-rapporteur>.
- The Palestine Chronicle. 'Israeli Firms Turn Connected Cars into Surveillance Tools – Israeli Media'. 18 February 2026. <https://www.palestinechronicle.com/israeli-firms-turn-connected-cars-into-surveillance-tools-haaretz-investigation/>.
- The Times of Israel. 'Israel Using AI to Pinpoint Hamas Leaders, Find Hostages in Gaza Tunnels — Report'. The Times of Israel, 26 April 2025. <https://www.timesofisrael.com/israel-using-ai-to-pinpoint-hamas-leaders-find-hostages-in-gaza-tunnels-report/>.
- Zureik, Elia. 'Colonialism, Surveillance, and Population Control'. In *Surveillance and Control in Israel/Palestine: Population, Territory, and Power*, edited by Elia Zureik, David Lyon, and Yasmeen Abu-Laban. Routledge Studies in Middle Eastern Politics 33. Routledge, 2011. <https://doi.org/10.4324/9780203845967>.
- Zureik, Elia, and David Lyon. 'Coronavirus Surveillance and Minority Groups in Israel/Palestine'. *The Middle East International Journal for Social Sciences* 3, no. 3 (2021): 197–215.
- Zureik, Elia T. *Israel's Colonial Project in Palestine: Brutal Pursuit*. Routledge Studies on the Arab-Israeli Conflict 20. Routledge, 201

Contact us:
info@7amleh.org | www.7amleh.org
Our social media pages: 7amleh

