



Israel's Surveillance Industry and Human Rights:

Impact on Palestinians

and Worldwide



7amleh - The Arab Center for the Advancement of Social Media
December 2023

Israel's Surveillance Industry and Human Rights: Impact on Palestinians and Worldwide

Contact us:

Email: info@7amleh.org

Website: www.7amleh.org

Telephone: +972 (0) 7740 20670

Find us on social media: 7amleh

Introduction

This report provides an overview of Israel's surveillance industry, outlines its impact on Palestinians' human rights, and details the industry's human rights implications worldwide. The analysis that follows draws from scholarly writing and policy briefs as well as previously published research on Palestinians living under intensive state surveillance in the West Bank and East Jerusalem. Five sections contextualize the growth of Israel's surveillance industry within global trends in securitization and surveillance at the start of the 21st century, examine the impact of spyware, social media monitoring, and biometric surveillance in Israel and the Occupied Palestinian Territories and worldwide, and offer recommendations to mitigate the harmful impacts of these systems.

Israeli surveillance of Palestinians across the region has proliferated since October 7th and the subsequent war on Gaza. As policing and military tactics developed over the last few days intensify, emergency measures have granted police and military personnel unchecked surveillance powers over Palestinians in Israel and the Occupied Palestinian Territory. By outlining a recent history of Israel's private surveillance industry and its impact on Palestinians in General and specifically those who live in East Jerusalem and West Bank, this report provides context and lends clarity to current events.

Innovations in first digital and then automated surveillance intensified the scope of Israeli surveillance of Palestinians in Israel and the Occupied Palestinian Territory at the start of the 21st century. Many of the technologies developed and refined in Occupied Palestinian Territory have subsequently fed into a burgeoning and global security homeland industry that prizes innovations in digital and automated surveillance. The three case studies discussed below demonstrate how the use of invasive surveillance technology on Palestinians has allowed Israeli firms to become private industry leaders, exporting invasive systems around the world. These examples also illustrate how new surveillance systems have a repressive impact on civilians living under intensive policing or military occupation. In Occupied Palestinian Territory, the systems discussed have exacerbated violence to the detriment of human rights. This report underscores how new surveillance technologies have eroded Palestinians fundamental right to privacy as well as their right to movement, right to assemble, and freedom of expression as enshrined by United Nations' Declaration of Human Rights.¹ By understanding the impact of new surveillance technologies in Israel and the Occupied Palestinian Territories and their global reverberations, this policy brief emphasizes the need to reign in the development, deployment, and export of new systems.

Background

Israeli military surveillance of Palestinians has a long history that stretches well beyond 1948, when 750,000 Palestinians were expelled from their homes and Israel subjected those who remained to a military rule marked by pervasive surveillance.² As Palestinian historians have noted, Israel's annexation and subsequent occupation of Palestinian territory (the West Bank, East Jerusalem, and Gaza) in 1967 extended these practices beyond the 1949 armistice line.³ For decades, Israeli spying, wiretapping, and aerial reconnaissance has eroded the fundamental human rights of Palestinians in Israel and the Occupied Palestinian Territory. Yet Israel emerged as a global leader in surveillance technology at the turn of the 21st century. It was the dawn of what Shoshanna Zuboff calls surveillance capitalism, a profit-making system predicated on expropriating tech users' data.⁴ Surveillance capitalism was pioneered through state-corporate partnerships in the United States following the events of September 11, 2001, and the advent of a global war on terror. The U.S. government traded scant regulations on growing technology firms for access to their vast reserves of users' private data, all in a bid to keep up with the surveillance capacities of a civilian technology sector. Yale Law

1 Nations, United. n.d. "Universal Declaration of Human Rights." United Nations. United Nations. Accessed December 5, 2023. <https://www.un.org/en/about-us/universal-declaration-of-human-rights>.

2 Sa'di, Ahmad. 2016. *Thorough Surveillance: The Genesis of Israeli Policies of Population Management, Surveillance and Political Control towards the Palestinian Minority*. Manchester, UK: Manchester University Press.

3 Zureik, Elia. 2016. *Israel's Colonial Project in Palestine: Brutal Pursuit*. London: Routledge.

4 Zuboff, Shoshanna. 2019. *The Age of Surveillance Capitalism*. New York: Hachette Books. <https://www.hachettebookgroup.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395694/?lens=publicaffairs>.

Professor Jack Balkin suggests that the U.S.'s anti-regulation stance turned the internet and the private companies capitalizing on surveilling it into a lawless space.⁵ Private companies devoted to data harvesting and analysis proliferated, supplying tools and expertise to the government in exchange for weak regulatory oversight.

Like many other countries, Israel learned from the U.S.' model of state surveillance and corporate profit-making.⁶ Heads of Israel's intelligence community consulted with U.S. security experts and technology CEOs to significantly expand Israel's intelligence apparatus across the occupied West Bank, East Jerusalem, and Gaza to meet the demands of the digital era. It was also the tail end of the second intifada, and Israel's military embraced dragnet surveillance as a deterrence mechanism, a tactic to avert more violence instead of lasting political solutions. Units like 8200, Israel's version of the NSA, grew from passive signal intelligence units into what generals described as a collection of 'mini-start-ups' boasting more soldiers than the navy.⁷ The military trained conscripts in offensive hacking, technological development, and data analysis. Israel's military denies Palestinian civilians living under occupation a right to privacy, creating a stark discrepancy from the rights granted to Israeli citizens. Soldiers gained experience building up and managing cutting-edge surveillance and security technologies with minimal limitations on who they could surveil and what kind of data they might collect.⁸

The expansion of Israel's military surveillance apparatus in the West Bank fueled the rapid development of the country's high-tech economy. Close ties between the army and private technology industry had been established decades earlier, seeding a robust technology sector primarily led by veterans of Israeli military intelligence units. However, as Israeli sociologist Neve Gordon notes, Israel's high-tech industries experienced unprecedented growth following 9/11, as demand for security and surveillance tech soared worldwide.⁹ Israeli startups experimenting with artificial intelligence, data analysis, and cyber espionage proliferated. Alliances between Israel and the U.S. meant that the U.S. military, CIA, and FBI were Israeli surveillance firms' frequent customers. By 2016, Israel was home to the most surveillance companies per capita in the world and considered a global 'homeland security capital.'¹⁰ In turn, as the Palestinian Coalition for Digital Rights notes, Occupied Palestinian Territory became a "testing ground for oppressive regimes and technologies."¹¹

Human rights abuse scandals have surrounded Israel's surveillance industry in recent years and are discussed below. Nonetheless, Israel's surveillance industry is booming. According to the Carnegie Endowment, as of summer 2023, Israel remains the leading exporter of spyware and digital forensic technologies.¹² Of the 74 governments that buy this surveillance technology from private vendors, 54 countries have purchased from Israeli surveillance firms. In October 2023, Haaretz reported that Israeli arms and cyber sales had skyrocketed in the past few years to an all-time high.¹³

5 Balkin, Jack M. 2017. "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation." SSRN Electronic Journal. <https://doi.org/10.2139/ssrn.3038939>.

6 Goodfriend, Sophia. 2022. "Supply and Demand: The U.S.' Impact on Israel's Surveillance Sector." 7amleh: The Arab Center for the Advancement of Social Media.

7 Goodfriend. 2022. "Point. Click. Occupy." The Baffler, September 12, 2022. <https://thebaffler.com/latest/point-click-occupy-goodfriend>.

8 Beaumont, Peter. 2014. "Israel's Unit 8200 Refuseniks: 'You Can't Run from Responsibility.'" The Guardian, September 12, 2014, sec. World news. <https://www.theguardian.com/world/2014/sep/12/israel-unit-8200-refuseniks-transcript-interview>.

9 Gordon, Neve. 2010. "Israel's Emergence as a Homeland Security Capital." In *Surveillance and Control in Israel/Palestine*. London: Routledge.

10 "The Global Surveillance Industry." 2016. Privacy International. https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

11 "The Palestinian Digital Rights Coalition Welcomes the Filing of a Lawsuit against the Israeli Surveillance Tech NSO Group." n.d. Al-Haq. Accessed December 6, 2023. <https://www.alhaq.org/advocacy/19810.html>.

12 Kot, Steven Feldstein, Brian (Chun Hey). 2023. "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Carnegie Endowment for International Peace. Accessed October 4, 2023. <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229>.

13 Yaron, Oded. October 2 2023. «Record-Breaking Spike in Countries Buying Israeli Arms and Cyber.» Haaretz. <https://www.haaretz.com/israel-news/security-aviation/2023-10-02/ty-article/.premium/number-of-countries-israel-sells-arms-and-cyber-to-spikes/0000018a-ea37-d3af-a3ce-ebf75d210000>.

Occupied Palestinian Territory as Laboratory

Since the early 2000s, Israeli politicians have claimed that spyware, biometrics, drone reconnaissance, and CCTV surveillance developed by private Israeli firms bolsters Israel's military capacity, as the army often outsources research and development to private firms.¹⁴ Industry leaders also claim private firms in Israel can rely upon their close relationship with the IDF to advance research, development, and implementation of new technologies. As part of the "dual feeding" process, elite military intelligence units recruit talented high school graduates for military service, where they receive significant training and experience.¹⁵ Once their mandatory service is up, many join startup companies or establish their own, often in cybersecurity or AI.

As Israel's surveillance infrastructure expanded across the West Bank, East Jerusalem, and Gaza Strip over the past two decades, Palestinian advocates, journalists, and academics warned the military was exploiting the occupation to test and refine new technologies sold on global markets. Israeli civilians are guaranteed robust privacy protections under civil law. However, because Palestinian civilians living under military rule are denied recourse to civil rights protections by an occupying army, there are very few checks on how the military deploys surveillance technologies in the occupied territories.¹⁶ Remarking on this dynamic, scholars and human rights organizations have recently suggested that Palestinians offer up a cheap reserve of raw data for private companies eager to test out and refine surveillance systems before exporting them abroad.¹⁷

Occupied Palestinian Territory has long been framed as a testing ground for Israeli weapons and security products. Israel has consistently ranked among the top ten arms-exporting countries for the past 50 years.¹⁸ Before digital and automated surveillance, the country was known for selling Uzi Machine Guns and Elbit tanks worldwide. The journalist Anthony Lowenstein links Israel's leading role in defense industries to its occupation of the West Bank, Gaza, and East Jerusalem in 1967. "Israel has developed a world-class weapons industry with equipment conveniently tested on occupied Palestinians, then marketed as 'battle-tested,'" Antony Loewenstein writes. "Cashing in on the IDF brand has successfully led to Israeli security companies being some of the most successful in the world."¹⁹ As Mona Shtaya has noted, the rise of a global surveillance industry was a boon to Israel's robust defense industry, fed by "surveillance technologies used on Palestinians."²⁰ Private firms devoted to electronic and internet monitoring increased from 2001 onward as NATO governments joined the so-called global war on terror. Yet, as the case studies below demonstrate, the development and deployment of surveillance technologies eroded Palestinians' fundamental human rights and had similarly damaging impacts abroad.

14 Melman, Yossi. 2022. "A Wild, Dangerous Military-Security Complex Has Seized Power in Israel." Haaretz, January 20, 2022, sec. Israel News. <https://www.haaretz.com/israel-news/2022-01-20/ty-article-opinion/a-wild-dangerous-military-security-complex-has-seized-power-in-israel/0000017f-f1b3-df98-a5ff-f3bf79b00000>.

15 Mhajne, Anwar. 2023. "Israel's AI Revolution: From Innovation to Occupation." Carnegie Endowment for International Peace. Accessed November 16, 2023. <https://carnegieendowment.org/sada/90892>.

16 Goodfriend, Sophia. 2022. "How the Occupation Fuels Tel Aviv's Booming AI Sector." Foreign Policy (blog). February 21, 2022. <https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/>.

17 "Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians in the OPT." 2023. <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>.

18 Labarge, Blair L. 1988. "The Israeli Defense Industry: Limits to Growth?" *The Fletcher Forum* 12 (2): 341–58.

19 Lowenstein, Anthony. 2023. *The Palestine Laboratory*. New York, N.Y: Verso Books, 11

20 Shtaya, Mona. 2021. "Palestine Under Surveillance with Mona Shtaya." Al-Shabaka (blog). Accessed December 6, 2023. <https://al-shabaka.org/podcasts/palestine-under-surveillance-with-mona-shtaya/>.

Case Studies

1. Spyware

Spyware is malicious software that can be covertly installed onto computing devices; the most potent systems can access every facet of an operating system, stealing texts, recording calls, culling through emails, and even turning on cameras or microphones to record conversations. Once monopolized by technologically advanced military, today, armies and police forces worldwide can buy the technology from private vendors. Israeli firms are prominent in the global spyware industry, as veterans from elite intelligence units have brought technical skills and expertise to the private sector over the past few years. In turn critics have warned the proliferation of private spyware firms poses a threat to the right to privacy worldwide.

The ties between private cyber firms and Israel's military rule over the occupied Palestinian territories came under global scrutiny in the summer and fall of 2021. A series of articles across major news publications alleged spyware manufactured by the Israeli spyware firm the NSO Group had targeted thousands of dissidents, human rights workers, and opposition politicians around the world.²¹ Outrage over the abuse of the malware coalesced when the United States Department of Commerce blacklisted the NSO Group, among other spyware firms, banning them from trading with American companies.²² While the NSO group's notoriety hinged on its role in exporting Israeli cyber technology to autocratic regimes worldwide, it would become apparent the firm was also central to Israel's surveillance arsenal in Palestine. In November 2021, human rights investigators found the NSO Group's spyware on the phones of six Palestinian civil rights advocates and three senior Palestinian Authority officials.²³

The revelations came just weeks after the Israeli military accused six Palestinian human rights organizations, where three of the hacked civilians worked, of terrorism. Human Rights Watch said the revelations of spyware demonstrated how the Israeli military's surveillance of Palestinians violates their "fundamental right to privacy, undermines their freedom of expression and association, and threatens their security and their lives." The proliferation of invasive spyware also creates a "chilling effect on advocates or journalists who may self-censor out of fear of potential surveillance."²⁴ Those hacked recounted sleepless nights marked by anxiety that their phones had been recording intimate conversations with loved ones and children and worried anything they did or said had been taken out of context and would be used as grounds for arrest.²⁵ As Ubai al-Aboudi, executive director of the Bisan Centre for Research and Development, told Aljazeera. "This is more than just eavesdropping, it's terrifying. The spyware takes complete control over the phone. It can make calls to anybody, send messages and it can download content."²⁶ Such testimonies echo the narratives of human rights defenders around the world targeted by NSO Group's potent technology.²⁷

The NSO Group is not the only Israeli company that has and continues to develop and export the technology

21 Washington Post. 2021. "Takeaways from the Pegasus Project," July 18, 2021, sec. Investigations. <https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/>.

22 Lyngaas, Sean. 2021. "US Blacklists Israeli Firm NSO Group for Use of Spyware | CNN Business." CNN. November 3, 2021. <https://www.cnn.com/2021/11/03/tech/nso-group-us-blacklist/index.html>.

23 Kirchgaessner, Stephanie, and Michael Safi. 2021. "Palestinian Activists' Mobile Phones Hacked Using NSO Spyware, Says Report." The Guardian, November 8, 2021, sec. World news. <https://www.theguardian.com/world/2021/nov/08/palestinian-activists-mobile-phones-hacked-by-nso-says-report>.

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

25 Bajak, Frank, and Joseph Krauss. 2021. "Report: NSO Spyware Found on 6 Palestinian Activists' Phones." AP News. November 8, 2021. <https://apnews.com/article/technology-business-israel-jamal-khashoggi-hacking-6bfc5bc992de7f33f-5c8e969e69ce15c>.

26 Staff, Al Jazeera. 14 Nov. 2021. "Palestinian Rights Activists Defiant over Israeli Spyware Hacks." Al Jazeera. Accessed December 6, 2023. <https://www.aljazeera.com/news/2021/11/14/palestinian-rights-activists-defiant-over-israeli-spyware-hacks>.

27 Carey, Matthew. 2021. "'Terror Contagion' Director Laura Poitras On Dangers Of Israeli Company's Pegasus Malware: 'It's Classified As A Cyber Weapon.'" Deadline (blog). December 11, 2021. <https://deadline.com/2021/12/terror-contagion-neon-short-documentary-director-laura-poitras-interview-news-1234889177/>.

worldwide. In 2021, malware manufactured by the Israeli firm Candiru was found on the phones of politicians, journalists, and scholars in Iran, Yemen, Israel, the United Kingdom, and Turkey.²⁸ Spyware manufactured by Cytrox, an Israeli firm based in Athens, infected the phones of journalists in Egypt and the E.U. in 2021 and 2022. Quadream, whose tools have been sold to Saudi Arabia, manufactured spyware that was found on human rights defenders' and journalists' phones worldwide in 2023.²⁹

The ties between these companies and the Israeli military cannot be understated. In 2018, Haaretz reported that 80 percent of the 2,300 people who founded Israel's 700 cyber companies were veterans of IDF intelligence units.³⁰ In 2021, the New York Times found that nearly every member of NSO Group's research team had worked at the Israeli Military Intelligence Directorate. Similarly, the founders of other major Israeli spyware firms like Candiru, Intellexa, and Cytrox served in leadership roles within Israel's military intelligence, some of whom were responsible for developing and deploying cyberweapons across the occupied Palestinian territories.³¹

Collaborations between the private spyware industry and the military exceed professional networks. The military outsources much of its technological development to private cybersecurity firms. In turn, fledgling surveillance companies gain an opportunity to refine their products before exporting them abroad, testing invasive and virtually unregulated surveillance systems on Palestinian civilians living under Israeli military rule. This reciprocal relationship paved the way for lenient export controls on companies like the NSO Group, whose products would double as diplomatic cards in regional geopolitical games. Israeli diplomatic gains—establishing formal relationships with countries throughout the MENA region, for example—were often preceded by NSO Group sales.³²

The NSO Group's reputation was ruined after the 2021 revelations, thanks to the collaborative work of investigative journalists worldwide. Israel pledged to adopt stricter export regulations, limiting what products Israeli firms could sell to foreign governments. In April 2023, Calcalist reported Israel's spyware industry shrunk rapidly in recent years. Many Israel-based firms had moved overseas or, if they remained, changed their focus.³³ Nevertheless, Israel's government has maintained close ties with shunned groups like the NSO Group or Candiru. Israel's security services made use of both firms' products after the war with Gaza erupted on October 7, in a move that constituted a stark reversal of previous policies.³⁴ The NSO Group and Candiru have since branded themselves as volunteers in the Israeli war effort, offering their systems to locate Israeli hostages inside Gaza and indicating that long-standing relationships between Israeli officials and the maligned companies were never ruptured.³⁵ According to documents obtained by the Intercept, the NSO

28 Megiddo, Gur. 2021. "We're on the U.S. Blacklist Because of You': The Dirty Clash between Israeli Cyberarms Makers." Haaretz, December 17, 2021, sec. Israel News. <https://www.haaretz.com/israel-news/2021-12-17/ty-article-magazine/highlight/were-on-the-u-s-blacklist-because-of-you-the-clash-of-israeli-cyberarms-firms/0000017f-f195-dc28-a17f-fd-b72e9a0000>.

29 Kabir, Omer. 2023. "Is Israeli Spyware a Dying Sector?" Ctech. April 20, 2023. <https://www.calcalistech.com/ctechnews/article/twccg3tql>.

30 Shezaf, Hagar, and Jonathon Jacobson. 2018. "Revealed: Israel's Cyber-Spy Industry Helps World Dictators Hunt Dissidents and Gays - Israel News - Haaretz.Com." Haaretz, October 20, 2018. <https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdad-de240000>.

31 Kot, Steven Feldstein, Brian (Chun Hey). n.d. "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses." Carnegie Endowment for International Peace. Accessed November 16, 2023. <https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229>.

32 Bergman, Ronen, and Mark Mazzetti. 2022. "The Battle for the World's Most Powerful Cyberweapon." The New York Times, January 28, 2022, sec. Magazine. <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html>.

33 Kabir, Omer. 2023. "Is Israeli Spyware a Dying Sector?" Ctech. April 20, 2023. <https://www.calcalistech.com/ctechnews/article/twccg3tql>.

34 Newman, Marissa. 2023. "Israel Taps Blacklisted Pegasus Maker to Track Hostages in Gaza." Bloomberg.Com, October 26, 2023. <https://www.bloomberg.com/news/articles/2023-10-26/israel-taps-blacklisted-pegasus-maker-nso-to-track-gaza-hostages-and-hamas>.

35 Ackerman, Gwen, and Marissa Newman. n.d. "Israel Is Using Pegasus Spyware Maker to Track Hostages in Gaza Bloomberg." Accessed December 14, 2023. <https://www.bloomberg.com/news/articles/2023-10-26/israel-taps-blacklisted-pegasus-maker-nso-to-track-gaza-hostages-and-hamas>

Group has also offered its services to the United States government.³⁶ How the industry responds to the war in the region remains to be seen. One thing is clear: Israel's use of the technology against Palestinians fed into the proliferation of systems that have eroded the right to privacy in most contexts they are deployed.

2. Social Media Surveillance

Social media became key to Israel's surveillance of the occupied Palestinian territories as soon as they became widely available in the region in the late 2000s. The Arab Spring made platforms like Facebook, Instagram, and TikTok integral to widespread protests across the Middle East, including Palestine. In turn, Israel's military intelligence developed more invasive ways of monitoring Palestinian digital spaces—from predictive policing algorithms to social media scraping bots that pinpoint and flag supposedly incendiary content.³⁷ Reporters note this sophisticated surveillance arsenal works in tandem with discriminatory incitement laws that criminalize much Palestinian political speech.³⁸ In 2016, Israel's parliament broadened the legal definition of incitement to encompass not only speech that “directly calls for violence” but also speech that, in the judgment of prosecutors, “expresses support for terrorist acts,” with or without a resolution to carry them out.³⁹

Israel's military has relied on both passive and active social media monitoring to police Palestinian digital spheres. Passive surveillance makes use of social media scraping tools to comb through Palestinian content, increasingly using A.I. to analyze data, identify criminal content, and predict which users are likely to violate Israeli laws and regulations. Recent reporting suggests these predictive policing algorithms have a very low accuracy rate.⁴⁰ Active surveillance entails using generative A.I. to create fake profiles that spread disinformation, propaganda, and software that can hack into private accounts. In 2018, Haaretz reported that these efforts had been consolidated under the “Center for Consciousness Operations,” a unit unveiled to wage covert psychological operations online, targeting both the occupied territories and worldwide.⁴¹ In the aftermath of the 2021 war between Israel and Hamas, spurred by historic protests in occupied East Jerusalem, also known as the Unity Intifada or Sheikh Jarrah uprising, Haaretz alleged Israel's security services relied on avatars to disseminate fake news across social media and encrypted messaging apps, including Telegram.⁴² Israel's military and security services also use A.I. to police and flag Palestinian social media content.

In 2023, the head of Israel's security services said AI was a “co-pilot” in carrying out IDF operations.⁴³ The increasingly high-tech nature of social media surveillance comes amidst reports of heightened repression against Palestinians and the eroding of fundamental rights like freedom of expression and the right to assemble. According to 972 Magazine, detentions and arrests due to social media posts have risen in recent years, especially for Palestinian Jerusalemites.⁴⁴

36 Gee, Georgia. 2023. “Israeli Spyware Firm NSO Demands ‘Urgent’ Meeting With Blinken Amid Gaza War Lobbying Effort.” The Intercept. November 10, 2023. <https://theintercept.com/2023/11/10/nso-group-israel-gaza-blacklist/>.

37 Fatafta, Marwa, and Nadim Nashif. 2017. “Surveillance of Palestinians and the Fight for Digital Rights.” Al-Shabaka (blog). Accessed December 6, 2023. <https://al-shabaka.org/briefs/surveillance-palestinians-fight-digital-rights/>.

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

39 “Israel's New Counter-Terrorism Law and Terrorism in Cyberspace.” n.d. Council on Foreign Relations. Accessed November 16, 2023. <https://www.cfr.org/blog/israels-new-counter-terrorism-law-and-terrorism-cyberspace>.

40 “Study Finds Predictive Policing Software Is Actually Pretty Terrible at Predicting Crimes.” 2023. Gizmodo. October 3, 2023. <https://gizmodo.com/predictive-policing-cops-law-enforcement-predpol-1850893951>.

41 Harel, Amos. 2018. “Israeli Army Sets Up ‘Consciousness Ops’ Unit to Influence Enemy Armies, Foreign Media and Public Opinion.” Haaretz. March 10, 2018. <https://www.haaretz.com/israel-news/2018-03-10/ty-article/with-eye-on-hearts-and-minds-israeli-army-sets-up-consciousness-ops/0000017f-eff4-d223-a97f-effdab210000>.

42 “Study Finds Predictive Policing Software Is Actually Pretty Terrible at Predicting Crimes.” 2023. Gizmodo. October 3, 2023. <https://gizmodo.com/predictive-policing-cops-law-enforcement-predpol-1850893951>.

43 Reuters. 2023. “Israel's Shin Bet Spy Service Uses Generative AI to Thwart Threats | Reuters,” June 27, 2023. <https://www.reuters.com/technology/israels-shin-bet-spy-service-uses-generative-ai-thwart-threats-2023-06-27/>.

44 Reiff, Ben. 2023. “For Palestinians, Social Media Influence Comes with the Threat of Prison.” +972 Magazine. October 2, 2023. <https://www.972mag.com/palestinian-influencers-social-media-persecution/>.

A 2021 report by 7amleh reported many young Palestinians felt like the proliferation of surveillance on and offline amounted to another kind of incarceration.⁴⁵ Recent reporting has emphasized how social media surveillance is only intensifying since Israel's war on Gaza began.⁴⁶ In November, Israel's parliament introduced an amendment to the counterterrorism law that criminalizes 'consumption of terrorist media.' Palestinians in the West Bank, Palestinian citizens of Israel, and Palestinian Jerusalemites have all been subjected to ramped up surveillance as new legislation has further criminalized Palestinians' activity online. Legal experts say this kind of dragnet surveillance has a chilling effect on Palestinians across the region.⁴⁷ According to Adalah, "these measures together constitute a draconian crackdown on the free speech rights of Palestinians and political persecution against them as a group."⁴⁸

In recent years, Israeli-based surveillance firms have sold similar technologies on the private market. Some of these firms have been accused of extralegally stealing social media users' data and harvesting it for profit. In 2018, Meta sued the Israeli firm Voyageur Labs for allegedly using nearly 40,000 fake Facebook accounts to collect data on an estimated 600,000 users.⁴⁹ In 2020, Meta sued Israeli firm BrandTotal Ltd for illegally scraping personal data from users' accounts, including users' names, I.D., gender, date of birth, relationship status, and location information.⁵⁰ In 2023, Meta and X (formerly Twitter) sued the Israeli firm Bright Data for scraping and selling user content from Facebook, Instagram, and Twitter.⁵¹ This September, an investigation by Haaretz revealed that Israeli firms were also selling more invasive versions of these technologies as surveillance services to foreign countries.⁵² The investigation found that two firms, Insanet and Rayzone, had developed systems that not only scraped users' social media accounts but also infected users' phones by bypassing existing security protections to steal sensitive data. According to Haaretz, "former ranking members of Israel's defense establishment" and "serial entrepreneurs" in Israel's cyber industries founded these firms.

One such firm was embroiled in one of the more serious human rights scandals in recent years. Cambridge Analytica, the British consulting firm that stole millions of Facebook users' data to sway the results of democratic elections worldwide, reportedly worked with the Israeli cyber-mercenary firm Team Jorge, which is composed of veterans of Israeli intelligence units. While Cambridge Analytica ceased operations after being sued for illegal data harvesting by the United States Federal Trade Commission, Team Jorge continued to operate in secrecy. In 2023, a Forbidden Stories investigation revealed Team Jorge had meddled in African democratic elections for years. The firm reportedly sold disinformation software and hacking tools that breached political targets' emails and messaging accounts in Kenya and Nigeria in the late 2010s and early 2020s.⁵³ According to the Guardian, Team Jorge's founder, Tal Hanan, boasted of spreading disinformation

45 Goodfriend, Sophia, Bashar Bakri, and Rawan Sheikh Ahmad. 2021 "Intensification of Surveillance in East Jerusalem and Impact on Palestinian Residents' Rights: Summer and Fall 2021." Accessed November 17, 2023. <https://7amleh.org/2021/11/08/intensification-of-surveillance-in-east-jerusalem-and-impact-on-palestinian-residents-rights-summer-and-fall-2021>.

46 Kermanitzer, Mordechai. 2023. "קראת - ינוחטיב ינידמ - מיברע מיתרוזא תפידרל שמשל לולע רורט ימוטרפ לש הכירצ רסואה קוחה." Haaretz. October 25, 2023. <https://www.haaretz.co.il/news/politics/2023-10-25/ty-article/0000018b-676d-d326-a39b-677d1e110000>.

47 "Israeli Knesset Passes Draconian Amendment to the Counter-Terrorism Law Criminalizing - Adalah." n.d. Accessed November 17, 2023. <https://www.adalah.org/en/content/view/10951>.

48 "Crackdown on Freedom of Speech of Palestinian Citizens of Israel." 23 Oct. 2023 Adalah: The Legal Center for Arab Minority Rights in Israel. Accessed December 6, 2023. <https://www.adalah.org/en/content/view/10925>.

49 Bhuiyan, Johana. 2023. "NYPD Spent Millions to Contract with Firm Banned by Meta for Fake Profiles." The Guardian, September 8, 2023, sec. US news. <https://www.theguardian.com/us-news/2023/sep/08/new-york-police-tracking-voyager-labs-meta-contract>.

50 Whittaker, Zack. 2020. "Facebook Sues Two Companies Engaged in Data Scraping Operations." TechCrunch (blog). October 1, 2020. <https://techcrunch.com/2020/10/01/facebook-sues-two-companies-engaged-in-data-scraping-operations/>.

51 Wrobel, Sharon. 2023. "Musk's X Corp Sues Israel's Bright Data for Scraping Data." Times of Israel. July 27, 2023. <https://www.timesofisrael.com/musks-x-corp-sues-israels-bright-data-for-illegally-scraping-data/>.

52 Benjakob, Omer. 2023. "Revealed: Israeli Cyber Firms Have Developed an 'insane' New Spyware Tool. No Defense Exists." Haaretz, September 14, 2023, sec. Israel News. <https://www.haaretz.com/israel-news/2023-09-14/ty-article-magazine/highlight/revealed-israeli-cyber-firms-developed-an-insane-new-spyware-tool-no-defense-exists/0000018a-93cb-de77-a98f-ffdf2fb60000>.

53 Gur Meggido and Omer Benjakob. 2023. "The Israeli Hackers Who Tried to Steal Kenya's Election." Haaretz, February 15, 2023. <https://www.haaretz.com/israel-news/security-aviation/2023-02-15/ty-article-magazine/premium/the-israeli-hackers-who-tried-to-steal-kenyas-election/00000186-4b7f-d5d4-a5e7-ebff5c9c0000>.

during the 2019 elections in Senegal. Hanan allegedly claimed to have interfered in 33 presidential elections across the African continent.⁵⁴ Journalists have documented how this interference has infringed on freedom of expression and the right to privacy in every context such technology has been deployed.⁵⁵

The market for invasive social media surveillance technologies is booming. Israeli firms have been and continue to be critical players in this largely unregulated industry. Yet the chilling effect dragnet surveillance and disinformation have had on Palestinian social media users demonstrates the dangers of these technologies worldwide.

3. Facial recognition

Facial recognition cameras have recently spread across the West Bank and East Jerusalem, abetted by close collaborations with private facial recognition companies and the Israeli military. Yet the Israeli military's use of biometric surveillance is hardly new. Israel's military has mandated Palestinian permit holders to use biometric identification cards since the early 2000s, requiring those who study or work within Israel to hand over their biometric data to Israel's military.⁵⁶ The military's use of biometric surveillance expanded significantly with advancements in image processing and algorithmic surveillance. According to WhoProfits, Israeli police updated a network of CCTV cameras covering Jerusalem's old city with facial recognition capability in 2017.⁵⁷ By the late 2010s, Israeli authorities installed facial recognition cameras at major checkpoints leading into the occupied West Bank.

In 2019, investigative reporting also brought the ethics of biometric surveillance of Palestinians under global scrutiny. That same year, NBC revealed new facial recognition cameras were installed across East Jerusalem and hidden throughout the West Bank. Over the next few years, Israeli authorities would significantly expand their use of the technology. Investigative reporting on the Israeli military's practices in the occupied territories by the Washington Post in 2021 revealed soldiers were building up a biometric database—called Wolf-Pack—of all Palestinian civilians in the West Bank without their consent.⁵⁸ The database was connected to Blue Wolf, a mobile app installed on tablets soldiers carried when stationed in the West Bank. Importantly, the buildup of these systems rested on invasive practices that eroded civilian privacy, like pulling children out of bed to scan their faces and enroll them into a biometric database or stopping students on the way to school to scan their faces.⁵⁹ In 2023, Amnesty International and Breaking the Silence alleged that biometric surveillance had expanded to smaller checkpoints in the West Bank, including in Hebron.⁶⁰

Importantly, private companies worked with the military to build up and refine these systems. Advocate Issa Amro describes the Palestinian cities transformed by these new systems as “as a laboratory for (Israeli) security solution companies to...troubleshoot and market their technologies.”⁶¹ East Jerusalem's Mabat 2000 surveillance system was developed and installed by the Mer Group, an Israeli security firm that the IDF often

54 Kirchgaessner, Stephanie, and Jason Burke. 2023. “Political Aides Hacked by ‘Team Jorge’ in Run-up to Kenyan Election.” *The Guardian*, February 15, 2023, sec. World news. <https://www.theguardian.com/world/2023/feb/15/political-aides-hacked-by-team-jorge-in-run-up-to-kenyan-election>.

55 “In Nigeria, ‘Team Jorge’ Hackers Collaborated with Cambridge Analytica,” *Le Monde*. February 17, 2023. https://www.lemonde.fr/en/pixels/article/2023/02/17/in-nigeria-team-jorge-hackers-collaborated-with-cambridge-analytica_6016268_13.html.

56 Spektor, Michelle. 2020. “Imagining the Biometric Future: Debates Over National Biometric Identification in Israel.” *Science as Culture*; Abingdon 29 (1). <https://www.tandfonline-com.proxy.lib.duke.edu/doi/abs/10.1080/09505431.2019.1667969>.

57 “Big Brother in Jerusalem's Old City.” 2018. Who Profits. <https://www.whoprofits.org/writable/uploads/old/uploads/2018/11/surveil-final.pdf>

58 Dwoskin, Elizabeth. 2021. “Israel Escalates Surveillance of Palestinians with Facial Recognition Program in West Bank.” *Washington Post*, November 8, 2021. https://www.washingtonpost.com/world/middle_east/israel-palestinians-surveillance-facial-recognition/2021/11/05/3787bf42-26b2-11ec-8739-5cb6aba30a30_story.html.

59 Goodfriend, Automated State Violence

60 Shezaf, Hagar. 2023. “Israel Using Facial Recognition Technology to Entrench Apartheid, Amnesty International Says.” <https://www.haaretz.com/israel-news/2023-05-02/ty-article/.highlight/israel-using-facial-recognition-tech-to-entrench-apartheid-amnesty-intl-says/00000187-db8a-d9b4-abaf-fbbe6c080000?ts=1699971580597>.

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

contracts with.⁶² The Marker reported that the Israeli facial recognition firm Oosto (formerly AnyVision) manufactured and serviced biometric cameras at major checkpoints.⁶³ NBC also alleged the company had installed its cameras in East Jerusalem.⁶⁴ According to the Guardian, the Chinese firm Hikvision and TKH Security manufacture biometric cameras in Jerusalem and Hebron.⁶⁵ Hikvision has also been linked to the mass surveillance and incarceration of Uyghurs in Northwest China and is blacklisted by the United States Department of Commerce.⁶⁶

The Israeli army's implementation of biometric surveillance is part of an official move toward a "frictionless" occupation. Defense officials have promised new technologies would reduce dehumanizing interactions between soldiers and Palestinians, like strip searches and home invasions, by leaving identification up to machines rather than soldiers.⁶⁷ Yet major human rights organizations, researchers, and journalists contradicted these claims. Foreign Policy found that the implementation of automated surveillance increased the army's intrusion into the daily lives of Palestinians.⁶⁸ In Hebron, for example, the military-installed new cameras on Palestinians' rooftops. Soldiers would walk into private homes to service the systems, eroding privacy. In Jerusalem, researchers from Amnesty International described how the proliferation of cameras made many women worry the military was surveilling them even inside the privacy of their own homes.⁶⁹ Such findings corroborated a 2021 7amleh report that described how the proliferation of surveillance cameras made many Jerusalemites feel watched even inside and engage in self-policing, like remaining fully covered in street clothes and hijabs inside the privacy of their own homes.⁷⁰ Sociologist Nadera Shalhoub Kevorkian characterizes such surveillance as an "industry of terror" that engenders fear in those subjected to invasive surveillance mechanisms, especially women.⁷¹

The impact of these systems in Occupied Palestinian Territory suggests the biometric surveillance systems implemented in the name of reducing violence intensify insecurity for populations subjected to intensive policing and militarization by corroding a fundamental right to privacy. These findings contradict the claims of biometric startups, who promise the use of this tech will enhance security and reduce violence. Despite the questionable efficacy of these systems, governments and law enforcement agencies are increasingly embracing biometric surveillance, and Israeli firms are meeting this demand.⁷² However, these systems are simply yet another reminder that no form of occupation is safe and secure or acceptable for the Palestinian people, and that all people have the right to freedom from living under occupation and mass surveillance.

62 Who Profits, "Mabat 2000"

63 Ziv, Amitai. 2019. "Anivision: The Intriguing Israeli Start-up That Operates Secretly in the Territories." The Marker, July 14, 2019. <https://www.themarker.com/technation/2019-07-14/ty-article/.premium/0000017f-e19e-df7c-a5ff-e3fe311d0000>.

64 Solon. 2019. "Microsoft Funded Firm Doing Secret Israeli Surveillance on West Bank." NBC News, October 28, 2019. <https://www.nbcnews.com/news/all/why-did-microsoft-fund-israeli-firm-surveils-west-bank-palestinians-n1072116>.

65 Bhuiyan, Johana. 2023. "How Chinese Firm Linked to Repression of Uyghurs Aids Israeli Surveillance in West Bank." The Guardian, November 11, 2023, sec. Technology. <https://www.theguardian.com/technology/2023/nov/11/west-bank-palestinians-surveillance-cameras-hikvision>.

66 *ibid*

67 Goodfriend, "Automated State Violence."

68 "Automated Apartheid: How Facial Recognition Fragments, Segregates and Controls Palestinians in the OPT." 2023. Amnesty International. <https://www.amnesty.org/en/documents/mde15/6701/2023/en/>.

69 *ibid*

70 7amleh, "Intensification of Surveillance in East Jerusalem"

71 Shalhoub-Kevorkian, Nadera. 2015. Security Theology, Surveillance and the Politics of Fear. Cambridge Studies in Law and Society. Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9781316159927.11>.

72 Oosto maintains partnerships with governments and corporations across North America and Western Europe. According to investigative reporting by Disclose, the Israeli biometric startup Briefcam has been covertly supplying the French police with facial recognition cameras for eight years. Corsight AI provides police forces with body cameras equipped with facial recognition cameras.

Legal Analysis and Human Rights Implications

Under international law, Israel's military is an occupying power responsible for protecting the 'civil life' of Palestinians across the West Bank, East Jerusalem, and the Gaza Strip.⁷³ Yet the research and reporting summarized here indicate that spyware, social media monitoring, and facial recognition surveillance each constitute obtrusive restrictions on Palestinians that diminish civil life across the occupied territories. While new systems are rolled out under the auspices of "enhancing security" they systematically erode a right to privacy, assembly, movement and freedom of expression. The deployment of invasive surveillance systems on civilian populations has stifled Palestinian civil society while sharpening the repressive conditions of Israeli military rule—from those silenced by the fear that an occupying army is tapping their cell phones to those who worry soldiers will storm into their homes to build up a biometric database. Because the implementation of surveillance constitutes a systematic infringement on Palestinians fundamental human rights as outlined in the UN charter, the Israeli military's use of surveillance technologies on Palestinian civilians is contravening international law.

Legal experts and major human rights organizations have come to similar conclusions. In a 2020 report, the ICRC wrote new surveillance systems posed "potential humanitarian consequences" to civilian populations living under military occupation. Namely, "being targeted, arrested, facing ill-treatment...or suffering from psychological effects from the fear of being under surveillance."⁷⁴ In occupied East Jerusalem and the occupied West Bank, Amnesty International found that the expansion of surveillance "helps advance the unlawful security objectives of illegal settlers" by cementing Israeli control over Palestinians and eroding their right to movement, right to assemble, and freedom of expression.

This brief has gone one step further to demonstrate that the development and deployment of surveillance technologies across the occupied Palestinian territories is not only contrary to the interests of civilians living under decades of military rule; it is also detrimental to fundamental human rights around the world. Private Israeli firms omit the constraints of digital and AI-powered surveillance systems—the fear, insecurity, and repression—they enable in Occupied Palestinian Territory in branding strategies and advertisements. On global surveillance and security markets, spyware, social media monitoring, and biometric surveillance are branded as generic solutions to international insecurity, tried and tested in one of the world's most notorious conflict zones.

The human rights scandals embroiling many Israeli firms referenced in this memo are evidence of the inefficacy and dangers posed by the unregulated development and deployment of these systems worldwide. As in Palestine, the use of spyware, social media monitoring, and facial recognition surveillance by governments worldwide erodes the right to privacy, the right to assemble, the right to movement, and freedom of expression. From the NSO groups' terrorizing impact on journalists and civil society to the erosion of democratic processes abetted by social media surveillance firms like Team Jorge, these surveillance systems have not enhanced security in any context they are implemented. In many parts of the world, such technologies simply exacerbate violence.

73 <https://international-review.icrc.org/articles/ihl-hr-facial-recognition-technology-occupied-palestinian-territory-914>

74 Committee for the Red Cross. 2020 "Artificial Intelligence and Machine Learning in Armed Conflict: A Human-Centered Approach." International Review of the Red Cross, Vol. 102, No. 913, 2020, p. 4.69

Recommendations

Israel can take immediate steps to stop the harm of new surveillance technologies on Palestinians, including ceasing settlement construction and expansion, ending mass surveillance of innocent civilians, and the draconian policing of Palestinian digital spaces. 7amleh is hardly the first major human rights organization to offer such recommendations. In lieu of Israel adhering to these guidelines, let alone the stipulations of international law as outlined above, the international community can take concrete steps to reign in the development and deployment of invasive new technologies by private firms.

7amleh calls on countries to enact a comprehensive right-based legal framework for governing the use, development, and production of automated surveillance technologies and weaponry, as well as accountability mechanisms for bad actors from existing companies. Such legislation should put particular emphasis on protecting the privacy and other fundamental human rights of civilians. Drawing inspiration from the European Union's data protection legislation, such as the General Data Protection Regulation (GDPR), countries can implement privacy laws outlining the permissible scope of surveillance activities, authorize transparent data processing practices, and empower individuals with rights to access, rectify, and erase their personal data.⁷⁵ These legal safeguards will help prevent indiscriminate surveillance, while building accountability and ensuring that surveillance measures are proportionate, necessary, and subject to oversight. International bodies, like the United Nations, should continue to play a key role in facilitating collaboration towards rights-centered global norms and agreements on the responsible use of surveillance technologies, especially in conflict zones. Furthermore, as an important step towards enforcing rights-respecting norms, it is imperative that bad actors, who have caused harm, are held to account for their actions and business practices with regards to harmful surveillance technologies.

Countries should also implement comprehensive legal frameworks for the sale and export of such technologies. Calls for governments to reign in the sale and transfer of these systems are growing and have been endorsed by major human rights organizations and governing bodies, including the United Nations and the Red Cross.⁷⁶ While countries like the United States have blacklisted abusive companies, including the NSO Group and Candiru, targeting individual firms while allowing industry to operate without regulations will do little to mitigate the harmful impact of these technologies. International bodies should continue to mandate a comprehensive and global framework that regulates the sale and transfer of these systems. Furthermore, the sale of certain technologies should be banned altogether. The international community has come to agreement on multiple occasions that certain weapons are antithetical to the respect of human dignity. As surveillance technologies continue to be weaponized, it seems we are arriving at another such occasion. Such efforts can set an important example for Israel to do the same while also severely limiting how Israeli firms capitalizing on the occupation can operate.

75 "General Data Protection Regulation (GDPR) – Official Legal Text." 2016. Accessed December 6, 2023. <https://gdpr-info.eu/>.

76 UN Affairs. 2023. "UN and Red Cross Call for Restrictions on Autonomous Weapon Systems to Protect Humanity | UN News." UN News. October 5, 2023. <https://news.un.org/en/story/2023/10/1141922>.