Supply and Demand:
The U.S.' Impact on Israel's Surveillance Sector

July 2022

By Sophia Goodfriend

حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media

Supply and Demand: The U.S.' Impact on Israel's Surveillance Sector

Introduction

Earlier in 2022, Israel's surveillance sector drew international condemnation after news of their abusive practices plastered headlines. At that time, a consortium of journalists and civil society organizations alleged that Israeli spyware was used to target some 50,000 journalists, human rights defenders, and foreign heads of state around the world.[1] The Washington Post revealed Israel's military deployed facial recognition cameras and biometric databases to extensively monitor Palestinian civilians in the West Bank, contracting with private companies to extend its reach.[2] Today, international legal experts warn that Israeli surveillance technologies threaten human rights worldwide.[3]

While journalists, politicians, and human rights advocates often frame Israel's surveillance industry as exceptional, it did not develop in isolation. This report details the U.S.' impact on Israel's surveillance industry between 2002 and 2022. The research results are organized around three main points. First, the analysis details how Israel implemented a model of corporate-state surveillance, developed in the U.S. following 9/11 through formal collaborations between the two countries' security apparatuses. Second, the report examines the U.S.' anti-regulation stance towards technology

---

[1] Amnesty International. *Massive data leak reveals Israeli NSO spyware used to target activists, journalists, and political leaders*. Amnesty International. 9 July 2021 Accessed 12 May 2022 https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/

[2] Hendel, Jonathan. 3 May 2022. "The watchful eye of Israel's surveillance empire" *972 Magazine.* Accessed 18 May 2022: https://www.972mag.com/israel-surveillance-facial-recognition/

[3] DeSombre, Winona. Lars Gjevik, and Johann Ole Willers. "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets." *Atlantic Council.* Accessed 10 May 2022: https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/surveillance-technology-at-the-fair/#conclusion

companies detailing how U.S. companies and investors have poured millions into Israel's growing surveillance sector. Lastly, the research underscores the policy implications of the U.S.' influence over Israel's surveillance sector and outlines how U.S. lawmakers can set global regulatory standards. This report thus provides essential context and analysis to urgent conversations surrounding the use and abuse of new technologies.

Corporate-State Surveillance from the U.S. to Israel

Israel's surveillance sector took off in the early 2000s, shaped by a model of state-corporate surveillance pioneered in the U.S.. Harvard Sociologist Shoshanna Zuboff describes this time "as the dawn of surveillance capitalism," which she defines as an economic system that generates profit from technology users' personal data.[4] As U.S.-based technology giants like Google, Microsoft, Apple, and Meta came to dominate telecommunication services, they gained unprecedented access to users" information and cashed in on their ability to harvest and analyze private communications. In exchange for scant regulations on their operations, tech conglomerates often shared this data with the U.S. government, which struggled to keep up with civilian innovations.[5]

As Yale Law Professor Jack Balkin notes in his research on U.S. national security policy and new information technologies, by the late 2000s, public and private surveillance enterprises in the U.S. had become intertwined.[6] The events of 9/11 and ensuing War on Terror coupled with the rise of the digital economy spurred public intelligence agencies and private internet companies to

[4] Zuboff, Shoshanna. 2019. *The Age of SurveillanceCapitalism: The Fight for a Human Future at the New Frontier of Power.*Profile Books: New York.
[5] Ibid, 155.
[6] Balkin, Jack. 2008. "The Constitution in the National Security State." *Minnesota Law Review.* Accessed 17 May 2022. https://openyls.law.yale.edu/handle/20.500.13051/1545

develop complementary needs. The U.S. government, corporate conglomerates, and technology start-ups poured resources into developing advanced surveillance technologies to harvest users" data. This included mass surveillance tools, like facial recognition and social media scraping technology, as well as targeted monitoring, including spyware and signal jamming devices. Private companies supplied tools and expertise to the government and were subject to little regulatory oversight in return. The U.S.'s anti-regulation stance turned the internet, and the technologies developed to monitor it, into what experts describe as a lawless space.[7]

Many countries learned from the U.S. model of state surveillance and corporate profit making; Israel, the largest recipient of cumulative U.S. assistance since World War Two and a close ally to the U.S., is no exception.[8] Beginning in the early 2000s, 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.[9] 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"[10] that hosted more soldiers than the Israeli navy."[11] The military began training young conscripts in offensive hacking, technological development, and data analysis. Researchers note that Israel's intelligence units were able to develop cutting edge surveillance technologies to use on Palestinian civilians living under

[7] N.A. "The Wild West of Smart Phone Data." 2021. *Council on Foreign Relations.* Accessed 17 May. 2022. https://www.cfr.org/blog/wild-west-smartphone-data-and-surveillance
[8] N.A. 2022. "U.S. Foreign Aid to Israel." Congressional Research Service. Accessed 10 May 2022. https://sgp.fas.org/crs/mideast/RL33222.pdf.
[9] IMEU. (2021, November 29). Fact Sheet: Israeli Surveillance & Restrictions on Palestinian Movement | IMEU. Institute for Middle East Understanding (IMEU). Retrieved May, 2022, from https://imeu.org/article/fact-sheet-israeli-surveillance-restrictions-on-palestinian-movement
[10] Bar, Eli, Gabi Ayalon, Amnon Angor, and Zvi Fishler. "8200 State of Being: DNA or an Organizational Culture?" *Migdalor.* June 2007. (Hebrew)
[11] Adler, Seth. "Inside the Elite Israeli Military Unit 8200." *CyberSecurityHub.* 11 June 2020. Accessed 10 May 2022. https://www.cshub.com/threat-defense/articles/inside-the-elite-israeli-military-unit-8200

occupation because they are routinely denied privacy protections in the name of Israeli security concerns.[12] In turn, Israeli soldiers gained hands-on experience building up and managing new surveillance and security technologies as part of their military service and were eager to bring these new technologies and skill-sets to the private sector once discharged.

The expansion of Israel's military surveillance apparatus in the West Bank therefore fueled the rapid development of the country's high-tech economy. Relying on the close ties between the military and private technology industry which had been established decades earlier,[13] Israel's technology sector experienced unprecedented growth following 9/11, as demand for security and surveillance tech soared worldwide.[14] Primarily led by veterans of Israeli military intelligence units, Israeli start-ups 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.[15] By 2016, Israel was home to the most surveillance companies per capita in the world and considered a global 'homeland security capital.'[16]

Supply and Demand

[12] Talbot, Rohan. 2021. "Automating Occupation: International humanitarian and human rights law implications of the deployment of facial recognition technologies in the occupied Palestinian territory." *International Review of the Red Cross.* 102.914 (823-849).
[13] Maggor, Erez. 2020. "The Politics of Innovation Policy: Building Israel's 'Neo-Developmental State.' *Politics & Society.* (1-37)
[14] Gordon, Neve. 2010. "Israel's Emergence as a Homeland Security Capital". *in Surveillance and Control in Israel/Palestine. Population, Territory and Power.* Ed. Elia Zureik, David Lyon, Yasmeen Abu-Laban. London: Routledge Press).
[15] Greenwald, Glen.. "Cash, Weapons, and Surveillance: The U.S. Is a Key Party to Every Israeli Attack." The Intercept. 4 April 2014. Accessed March 31, 2022. https://theintercept.com/2014/08/04/cash-weapons-surveillance/.
Greenwald, Glenn, Laura Poitras, and Ewen MacAskill. 2013. "NSA Shares Raw Intelligence Including Americans' Data with Israel." *The Guardian.*
https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.
[16] N.A. "The Global Surveillance Industry." *Privacy International.* 2016. Accessed 17 May 2022.
https://privacyinternational.org/sites/default/files/2017-12/global_surveillance_0.pdf

The U.S' hands-off approach to regulating surveillance technology helped make U.S.-based venture capital funds and technology conglomerates some of the most prolific funders of private Israeli surveillance firms.[17] Meta, Microsoft, Google, Amazon, and Apple pioneered business models predicated on continuously tracking technology users on and offline. These companies have acquired more than 20 Israeli companies devoted to both mass data collection/analysis and targeted monitoring to date,[18] including firms that market biometric surveillance, cyberespionage, and data harvesting technologies.[19] Demand for more sophisticated surveillance technology means that U.S.-based venture capital funds have also poured millions into Israeli surveillance start-ups. Notable U.S.-based investors include Francisco Partners, which owns shares of the NSO Group,[20] Battery Ventures, funders of the Israeli spyware firm Paragon,[21] Andressen Horowitz, whose investments launched Israeli digital forensics firm Toka,[22] and LightSpeed Ventures, which owns shares of the biometric firm Oosto (formerly AnyVision).[23]

While many Israeli surveillance firms brand themselves as civilian companies, they often move fluidly between military and civilian contexts. In recent years, so-called 'dual use' surveillance technology has garnered intense criticism from advocates and lawmakers, who underscore the

[17] Kortum, S., & Lerner, J. (2000). Assessing the Contribution of Venture Capital to Innovation. The RAND Journal of Economics, 31(4), 674–692. https://doi.org/10.2307/2696354
[18] N.A. "Aquisitions by Google"; "Acquisitions by Meta"; "Aquisitions by Microsoft." ; "Aquisitions by Amazon" and "Aquisitions by Apple." *Tracxn.* N.D. Accessed 5 June 2022. https://tracxn.com/?redirect=false
[19] Christiansen, Siri. "Why All Investors Should be Concerned About Surveillance Technology." *CityWire.* 12 April 2022. Accessed 19 May 2022.
https://citywireselector.com/news/why-all-investors-should-be-concerned-about-surveillance-technology/a2384740
[20] Gilead, Asaf. "Squabbling Threatens NSO Sales." *Globes.* 29 Mar 2022. Accessed 5 May 2022.
https://en.globes.co.il/en/article-squabbling-threatens-15b-sale-of-nso-group-1001407395
[21]Brewster, Thomas. "Israeli Surveillance Startup That 'Hacks WhatsApp And Signal." *Forbes.* 29 July 2021. Accessed 5 May 2022.
https://www.forbes.com/sites/thomasbrewster/2021/07/29/paragon-is-an-nso-competitor-and-an-american-funded-israeli-surveillance-startup-that-hacks-encrypted-apps-like-whatsapp-and-signal/?sh=7d5832e3153b
[22] ibid
[23] N.A. "Lightspeed Venture Partners Invest in AI Leader to Accelerate Global Expansion." 14 January 2019. *Oosto.* Accessed 10 May 2022.

challenge of ensuring militaries or repressive regimes do not abuse surveillance tech.[24] For example, Oosto (formerly AnyVision), whose facial recognition cameras are installed at major Israeli army checkpoints in the West Bank, sells biometric cameras to "smart cities" in the U.S.. Microsoft was a major funder of the start-up in 2019 before pulling its investments following investigative reporting revealing the extent of the firms' collaborations with Israel's military, including installing facial recognition cameras in the West Bank and Jerusalem.[25] Despite Microsoft's divestment, Oosto continues to supply the Israeli army with facial recognition technology and exports its technology to municipalities in over 40 countries.[26]

As private firms like Oosto continue to attract millions from investors despite public condemnation, Silicon Valley is struggling to reign in a surveillance sector it played an outsized role in shaping. The rise and fall of the NSO Group, an Israeli cyberespionage firm that allegedly hacked the phones of 50,000 journalists, political dissidents, and politicians throughout its tenure, provides a clear example of this. The NSO group worked closely with Silicon Valley for most of its tenure: Meta was in talks to purchase NSO spyware, hoping to use its software to monitor users of its iOS mobile application in 2017.[27] Two years later, however, Meta reversed course and sued the company for accessing WhatsApp servers to install Pegasus, the NSO Group's trademark product, on targets' mobile devices. Apple followed suit in November 2021, announcing a lawsuit against the company

[24] Gildea, Ross James and Federica D'Alesandra. "We Need International Agreement on How to Handle These Dangerous Technologies. *Slate.com.* 7 March 2022. Accessed 17 May 2022. https://slate.com/technology/2022/03/dual-use-surveillance-technology-export-controls.html
[25] Solon, Alina. "Why did Microsoft fund an Israeli firm that surveils West Bank Palestinians?" *NBCnews.com.* October 29, 2019. Accessed 10 March 2022.
[26] Hempel, Jonathon. "The Watchful Eye of Israel's Surveillance Empire." *972 Magazine.* 3 May 2022. Accessed 17 May 2022. https://www.972mag.com/israel-surveillance-facial-recognition/
[27] Holmes, Aaron. "Facebook is Suing an Israeli Spyware Company." *Buisiness Insider.* 3 April 2020. Accessed 10 May 2022. https://www.businessinsider.com/nso-group-facebook-buy-pegasus-spyware-lawsuit-2020-4

shortly after revealing the firm hacked the phones of U.S. State Department officials in Uganda.[28] Upon receiving the news from Apple, the U.S. Department of Commerce placed the NSO Group and the Israeli spyware firm Candiru, along with four other surveillance companies, on a blacklist and barred the firms from doing business with U.S. entities. Alongside Meta and Google's high-profile lawsuits, the U.S. blacklisting pushed the NSO group to near bankruptcy. Israel's Defense Ministry responded by tightening its export regulations, forcing at least one other private surveillance firm to shut down.[29]

Despite these developments, NSO Group's collapse illustrates the limits of industry-led regulatory attempts. The NSO Group is just one of the hundreds of private spyware firms selling invasive military-grade espionage weapons to governments worldwide. Companies like the UAE-based Dark Matter recruit employees directly from the U.S. or Israeli intelligence agencies, promising lucrative salaries and benefits.[30] Other Israeli spyware firms are simply registering in countries with lenient export laws, like Cyprus or Northern Macedonia.[31] Such trends demonstrate how policies aimed at individual companies do little to curb the abusive practices of the entire private surveillance industry. Furthermore, corporate conglomerates like Meta and Google continue to invest in invasive surveillance technologies--particularly facial recognition and data harvesting

[28] Bergman, Ronen and Mark Mazetti. 28 January 2022. "The Battle for the World's Most Powerful CyberWeapon." *New York Magazine.* Accessed 15 April 2022.
https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html
[29] Gilead, Assaf. "Export Controls Strangling Israel's Attack Industry." *Globes.* 25 April 2022. Accessed 17 May 2022.
https://en.globes.co.il/en/article-tighter-export-controls-strangling-israels-cyberattack-sector-1001410066
[30] Mazzeti, Mark, Adam Goldman, Ronen Bergman, and Nicole Perlroth. "A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments." *The New York Times.* 21 March 2019. Accessed 18 May 2022.
https://www.nytimes.com/2019/03/21/us/politics/government-hackers-nso-darkmatter.html
[31] Benjakob, Omar. 19 April 2022. 'Great Alarm': First Detected Use of Mysterious Israeli Spyware on EU National.' *Haaretz.* Accessed 10 May 2022.
https://www.haaretz.com/israel-news/tech-news/israeli-predator-spyware-found-in-phone-of-top-greek-investigative-reporter-1.10748821

technologies whose abuse by governments and private firms are well documented. Despite announcing a new commitment to cracking down on the surveillance industry,[32] these companies play a pivotal role in funding surveillance technologies with zero accountability to users or regulatory oversight by domestic or international bodies.

Conclusion

This report has detailed how U.S. policy and corporate practices have influenced Israel's surveillance sector. Collaboration between Silicon Valley and the U.S. government allowed tech conglomerates and private funds to invest in intrusive surveillance technology free of accountability or oversight. Beginning in the early 2000s, Israeli start-ups raced to fill a growing demand for ever more innovative means of monitoring and tracking populations. Many founders of these firms repurposed surveillance systems and technological know-how developed in Israel's military, which engages in mass surveillance of a civilian population denied recourse to proper privacy protections. U.S.-based corporate conglomerates and hedge funds operating with zero accountability or oversight bought up these invasive technologies. Their demand lay the groundwork for today's global private surveillance industry. While these same corporations are leading efforts to reign in the surveillance tech industry, industry-led solutions are limited. The U.S. and international organizations must do more to ensure robust privacy protections and restrictions on the sale and transfer of surveillance technology.

Recommendations

[32] Dvilanski, Mike, David Agranovich, and Nathaniel Gleicher. December 2021. "Threat Report on the Surveillance-for-Hire Industry." *Meta.* Accessed 17 May 2022. https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf

The U.S. security establishment and U.S.-based technology companies have an outsized influence over Israel's surveillance sector. This means that the U.S. has the power to help stem the industry's abusive practices. The U.S. should establish comprehensive and far-reaching regulations to reign in the sale and transfer of both mass and targeted surveillance technologies. To date, the U.S. congress has failed to pass a single piece of comprehensive legislation protecting technology users and regulating technology conglomerates.[33] Legislation that bans indiscriminate mass surveillance by public and private entities alike, places limits on data collection by technology companies, and enshrines an overarching right to privacy at the federal level is more urgent than ever. These policies will curb the demand for more invasive surveillance technology and temper private investments in new companies.

Alongside federal laws, the U.S. should join efforts to establish broad and comprehensive international regulations on the sale and transfer of surveillance technologies worldwide. As private surveillance firms sell their products worldwide– to democratic governments, corporate conglomerates, and repressive regimes alike--the United Nations and a broad-based coalition of civil society organizations have called for overarching policies limiting their trade and use.[34] It is clear that limits on certain cyberweapons--like the U.S.' Blacklisting of Candiru and the NSO Group-- will not temper the risks posed by other AI-powered surveillance technologies, such as facial recognition technology and location monitoring. Therefore, it is essential that governments worldwide sign onto a binding and overarching export control regime that establishes permanent restrictions on the surveillance industry, particularly AI-powered surveillance technologies. The UN has demanded

[33] Kang, Cecilia. "As Europe Approves New Tech Laws the U.S. Falls Behind." *The New York Times.* 22 April 2022. Accessed 5 June 2022. https://www.nytimes.com/2022/04/22/technology/tech-regulation-europe-us.html
[34] N.A. "Spyware: Rights experts push for surveillance technology moratorium." *UN News: The United Nations.* Accessed 18 May 2022. https://news.un.org/en/story/2021/08/1097632

these controls ensure surveillance companies adhere to the UN Guiding Principles on Business and Human Rights, an important corporate accountability mechanism.[35] By joining efforts to establish and follow a global regulatory framework for surveillance technology, the U.S. can prevent new firms in Israel and beyond from developing more invasive technologies.

The struggle for digital rights in Palestine demonstrates the dangers unregulated surveillance poses worldwide. 7amleh has documented how Israel's unregulated use of CCTV surveillance, biometric monitoring, and intensive social media surveillance constrains Palestinians' freedom of speech, freedom of movement, and fundamental right to privacy.[36] Research demonstrates that, while Israeli officials often frame new surveillance technologies as humanitarian security solutions, these systems cause significant psychological damage and rely on intrusive policing practices.[37] U.S. policymakers must bring accountability to an industry that has operated with impunity for far too long, which can start with regulations and policy changes, as well as a commitment by U.S. companies and investment funds to stop fueling the dangerous surveillance industry, and take concrete steps to reign in the market.

---

[35] Keaten, Jamey and Matt O'Brien. "U.N. urges moratorium on use of AI that imperils human rights." *The LA Times.* 16 Sept 2021. Accessed 5 June 2022.
https://www.latimes.com/business/story/2021-09-16/u-n-urges-moratorium-on-use-of-ai-that-imperils-human-rights

[36] 7amleh. "Intensification of Surveillance in East Jerusalem and Impact of Palestinian Residents' Rights." *7amleh: The Arab Center for Social Media Advancement.*
https://7amleh.org/2021/11/08/intensification-of-surveillance-in-east-jerusalem-and-impact-on-palestinian-residents-rights-summer-and-fall-2021

[37] Goodfriend, Sophia. 21 February 2022. "How the Occupation Fuels Tel Aviv's Booming AI Sector." *Foreign Policy.* Accessed 10 May 2022. *https://foreignpolicy.com/2022/02/21/palestine-israel-ai-surveillance-tech-hebron-occupation-privacy/* and Shtaya, Mona. "Nowhere to Hide: The Impact of of Israel's Digital Surveillance Regime on Palestinians. The Middle East Institute. Acessed 5 June 2022.
https://www.mei.edu/publications/nowhere-hide-impact-israels-digital-surveillance-regime-palestinians


حملة – المركز العربي
لتطوير الإعلام الاجتماعي
7amleh - The Arab Center for
the Advancement of Social Media