The Accountability Paradox of Commercial Spyware: the NSO Group Case

28 OCTOBER 2026

Giulia Rossi



NSO Group Logo

1.400, this is the number of WhatsApp users who had their phones hacked by the Pegasus spyware and for which Meta started a long legal battle in October 2019. The malware was able to access private data by mimicking WhatsApp's server itself through phone calls to victims with different country code prefixes such as the Kingdom of Bahrain, the United Arab Emirates and Mexico. Consequently, Pegasus was able to take full control of the target's smartphones and all their stored information (Silberman, 2024). The NSO Group, an Israeli firm and developer of the spyware, continued to cause multiple system breaches throughout the six-year litigation process despite several court orders, with Meta's legal team alleging that the company deliberately defied the court's injunctions and demands (Simons, 2024).

This report examines whether accountability mechanisms are able to effectively constrain commercial spyware, or rather, they inadvertently legitimise it. In June 2026, Meta filed a contempt motion against NSO and,

shortly after, a member of the European Parliament's spyware investigation committee was targeted with Pegasus in July 2026. The analysis uses NSO Group as a case study through a qualitative review of court filings, lobbying disclosures and academic literature. While experts have addressed this tool's capabilities and human rights implications separately, this report argues that their structural interaction, specifically how legal and regulatory responses produce a paradox of legitimisation, remains underexplored. From the Meta litigation, through the Entity list dynamics, to NSO's ties with the State of Israel, the report delves into an original argument on the governance failure of commercial spyware.

The Court Litigation and Its Governmental Shadows

On February 23, 2024, Judge Phyllis J. Hamilton ordered NSO Group to *"produce information concerning the full functionality*" of the spyware and any other "remote access trojan" that the company developed (Lubin, 2024), on top of the original code of Pegasus. NSO argued that Israeli law prevents them from reproducing the code out of country and disclosing sensitive production information admissible at trial (Simons, 2024). However, leaked files from multiple media organisations revealed that in July 2020, Israeli officials had previously physically seized documents and equipment from NSO's offices in Tel Aviv, in order to prevent the company from complying with WhatsApp's eventual requests and transferring confidential documentation without explicit governmental authorisation (Davies et al., 2024).

The whole operation was under gag order, preventing the actions from being divulged. Scott Horton, lawyer and professor at Columbia Law School, described these as *"strange procedures to be taking in relation to a private entity",* suggesting NSO was in fact an *"integral part of the Israeli defence establishment"* (Davies et al., 2024). This last point is indicative of a foreign authority shielding a supposedly independent and private firm, de facto designating it as a national strategic asset, free from judicial oversight. Ultimately, the California jury ended up awarding over $167,000,000 in punitive damages and over $400,000 in compensatory damages to Meta (Novo, 2025), an unprecedented event for platform liability in the spyware industry.

In June 2026, the *WhatsApp v. NSO Group* regained public attention due to Meta accusing NSO of continuously violating the permanent injunction that banned them from operating on the network. The evidence of these illegal actions was 23 WhatsApp accounts and 34 groups identified as "test groups". Meta security engineer Andrew Blaich identified the clusters in at least 13 countries, with names explicitly referencing test operations in Sub-Saharan Africa, the Middle East and Central America (Mitra, 2026). According to the filing, through one-click links, NSO Group was capable of accessing classified material (Mitra, 2026).

These new accusations are only adding to the multiple controversies that the Israeli developer had to face before and during the many years of trial against WhatsApp. For instance, in a 2017 inquiry by The New York Times, it was reported that Mexico acquired Pegasus to investigate criminals and terrorists. Despite the initial claim, the targets turned out to mainly be HR lawyers, correspondents and anti-corruption activists (Silberman, 2024).

Lobbying as a response to blacklisting

The global reach of NSO's operations, combined with its demonstrated contempt for US court orders, prompted a regulatory response from Washington. In November 2021, under Biden's administration, the US Commerce Department added NSO Group and another Israeli commercial spyware company, Candiru (Lubin, 2024), to its Entity List, a federal blacklist which prohibits the exchange of American technologies. The official governmental statement explained this choice as proof of the administration's "*efforts to put human rights at the centre of U.S. foreign policy, including by working to stem the proliferation of digital tools used for repression.*" The press release further indicates that the NSO Group "*enabled foreign governments to conduct transnational repression* [...] *Such practices threaten the rules-based international order.*" (U.S. Department of Commerce, 2021).

From that moment on, an aggressive lobbying campaign began in order to remove NSO from the Entity List, principally since the presidential change. In 2025, Caroline Glick, a key advisor to Israeli prime minister Benjamin Netanyahu, was reported by Tel Aviv's media to be in the process of working with the Trump administration to lift the current sanctions (Ilnai, 2025). Moreover, in November of the same year, the company announced a new shareholder structure, with the consequent election of David Friedman as chairman (Panagiotopoulos, 2026). During his first term, Donald Trump described Friedman as a *"long-time friend and trusted adviser"* (Trump, 2016) thanks to his prior service as United States ambassador to Israel. It is therefore not a secret that Friedman intends to use his diplomatic ties to help restore Pegasus' reputation amongst American investors and US officials (Panagiotopoulos, 2026).

Another key aspect of NSO's rehabilitation strategy has been the Vogel Group, a Washington-based government affairs and consulting firm with direct ties to the Republican establishment and the Trump administration. In 2025, it was listed as Israel's software company's primary lobbying contractor (U.S. House of Representatives, 2026). While NSO's previous lobbying contractors were registered under the Foreign Agents Registration Act (FARA), which mandates detailed disclosure of any meetings or acts of influence by foreign governments and political parties, the Vogel Group registered under the Lobbying Disclosure Act (LDA), a significantly less transparent instrument that requires only broad quarterly reports with no obligation to specify whether the meetings are held for commercial

or diplomatic interests (Dennett, 2018). This shift from FARA to LDA, occurring precisely as Trump returned to the White House for his second term, confirms NSO Group as a direct client with a base in Israel, yet the content of that relationship remains largely shielded from public scrutiny by thoughtful design. Overall, the scale of this effort, at least $7.7 million in lobbying professionals and consultants between 2020 and 2025 (Lieber, 2025), clearly reflects something more than a private company seeking regulatory relief.

Perhaps the most revealing indicator of NSO's confidence in its political protection came in a rare interview to Israeli media dated December 2024, where NSO's co-founder Omri Lavie openly downplayed the impact of the Entity List designation: *"The Americans, when they say blacklist, it sounds much more dramatic to me than it actually is. You can still do business in the United States; it is definitely not a barrier for us to sell in the US. I strongly believe that what we are doing is important and essential both for the State of Israel and for the world*" (Frenkel, 2024). This declaration openly explains how a governmental regulatory tool like the Entity List has not fulfilled expectations and instead blurs the line between a private commercial enterprise and a sovereign tactical tool.

NSO's roots in Israeli State Infrastructure

Surveillance technology firms find in Israel a perfect ground to establish and flourish, making it the "Silicon Valley" of commercial spyware (Silberman, 2024). These private entities primarily recruit from MID graduates, most notably Unit 8200 alumni. The latter is a crucial asset to Israel's renowned cyber ecosystem, and each year approximately 1,000 top-notch cyber experts join the ranks of Israeli defence, industry and academia (Cohen et al., 2024). In recent years, due to the prestige of its cyber education, Unit 8200 talents have started to be more interested in the highly remunerative private sector of digital corporations like NSO, Cellebrite, Cytrox and Candiru (Ilnai, 2025).

The structural ties between NSO and the state of Israel, being intrinsically organisational, are a crucial apparatus when it comes to primary needs and protection of the country. The Ministry of Defence acquired Pegasus in 2013 and began operating with it in 2015 (Rubin, 2022). Years later, in 2022, Calcalist, Israel's leading economics newspaper, released an exclusive list of dozens of citizens and political figures who had reported having their devices hacked by Israeli police through Pegasus' malware (Ganon, 2022). The platform explained how these targets included anti-government protesters, senior parliament members, ministers and even Benjamin Netanyahu's entourage and family.

The revelation that Pegasus' zero-click spyware had been utilised by Israeli authorities for domestic law enforcement purposes caused massive turmoil in the Jewish state's society (Lubin, 2024), which, until that moment,

had assumed that such tools were mostly reserved for national security purposes (Rubin, 2022). Regarding this last aspect, since Hamas' attack on the 7th of October 2023, the Israel Defence Forces have partnered with NSO Group in order to strengthen surveillance in the Gaza Strip (Blessing, 2024). In a 2025 report to the UNHRC, Francesca Albanese, Special Rapporteur on the Occupied Palestinian Territories, explains how there's evidence of the spying malware being used to target Palestinian activists, leaders, journalists and human rights defenders who speak in favour of the recognition of the genocide (Albanese, 2025). Additionally, Pegasus has also been used to monitor phones in the West Bank, with the scope of retrieving vital information on Hamas members' locations and blackmailing fragile individuals (Gray, 2025). The malware has been employed in the field of other sensitive areas for the state of Israel, such as Iran, Lebanon and Yemen (Harwell et al, 2021). When questioned on the integrity of these actions towards Arabs and Palestinians, NSO's former CEO Hulio Shalev firmly stated: *"If Israel is using our tools to fight crime and terror, I would be very proud of it."* (Farrow, 2022).

With this level of premises, NSO's top product has easily become an alluring tool for most regimes around the world. Following the 2007 Defence Export Controls law, Israel's Ministry of Defence is designated as the only licensed institution able to decide whether and to whom to sell the country's cyberweapons outside domestic jurisdiction (Feldstein et al., 2023). Geopolitical events directly shape export licence decisions. When Ukraine tried in 2022 to acquire Pegasus, the whole operation was quickly shut down (Feldstein et al., 2023). Israeli officials did not want to undermine relations with Russia (Ward, 2023).

Human Rights Implication of Commercial Spyware

The consequences of selling such powerful spyware abroad are not abstract, but once Pegasus reaches its designated clients, Israel has no formal mechanism to supervise how it is deployed. A cross-analysis by Forbidden Stories and Amnesty International indicated a list of fifty thousand phone numbers that were targeted by a wide variety of countries with a history of human rights abuses and citizen surveillance (Amnesty International, 2021). Such countries are Azerbaijan, Bahrain, Hungary, India, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Togo, and the United Arab Emirates, which have all been identified as instigators of spying operations (De Martin, 2024). Said victims ranged from Arab royal family members, entrepreneurs, human rights advocates, writers, and more than 600 government officials (Amnesty International, 2021). One of the most infamous cases is the assassination of Washington Post reporter Jamal Khashoggi. After the killing, investigators found that the smartphones of the Saudi journalist's close associates had previously been infected with Pegasus (De Martin, 2024).

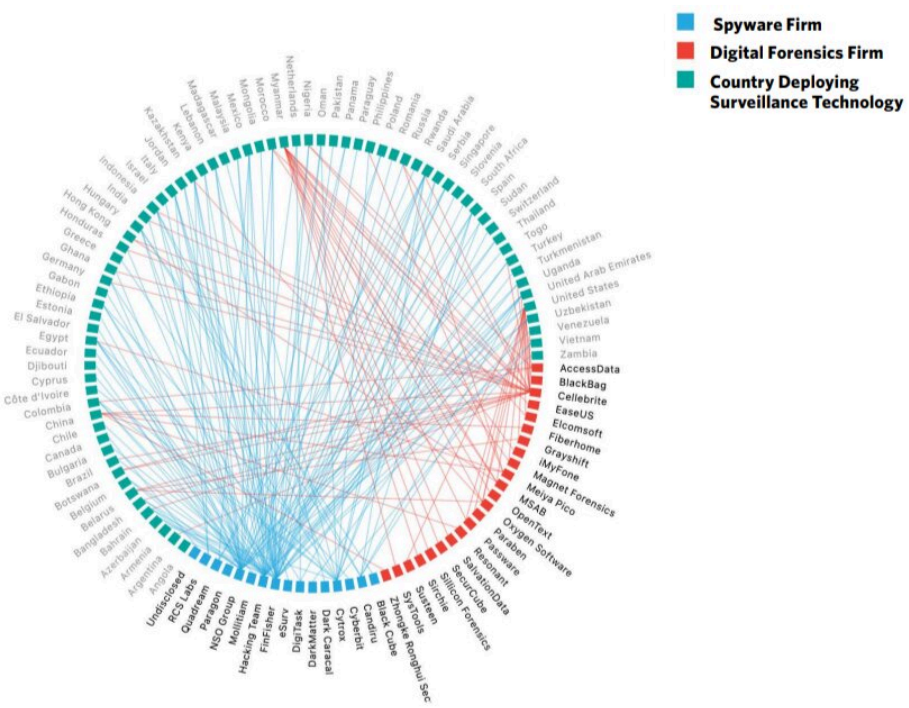


Figure 1. *Key Relationships between Governments and Intrusion Technology Firms.* Data source: *Carnegie Endowment for International Peace (2023). Available at:* https://carnegieendowment.org/features/commercial-spyware

While companies based in or connected to Israel have sold surveillance products to 56 of 74 identified governments active in the cyber trade between 2010 and 2023 (Feldstein et al., 2023), they are not the only ones in the global landscape. Major firms have rapidly joined the market, notably the Indian "BelltroX", the UAE "Crowdfense", the Italian "RCS Labs", and the French "Intellexa" (Lubin, 2024). Blacklisting companies who perpetrated infringement of human rights – like the US did with the Entity List – has proven to be ineffective.

The nature of the issue is rooted in the political economy of a sectoral market like intrusive technology (Feldstein et al., 2023), which is only destined to grow in demand. Policymakers' first objective would be to monitor the extensive exploitation of apparently lawful regulatory loopholes that spyware companies have used to avoid most accountability requirements. In fact, the practice of having subsidiaries under different names in countries that require little to no oversight, so-called regulatory havens (Farrow, 2022) – such as Hungary, Malta, Bulgaria, Singapore and Cyprus (Feldstein et al., 2023) – has become standard. And for every company branch blacklisted, less scrupulous successors are destined to emerge to fill the gap, perpetuating an accountability problem that endangers fundamental rights (Silberman, 2024).

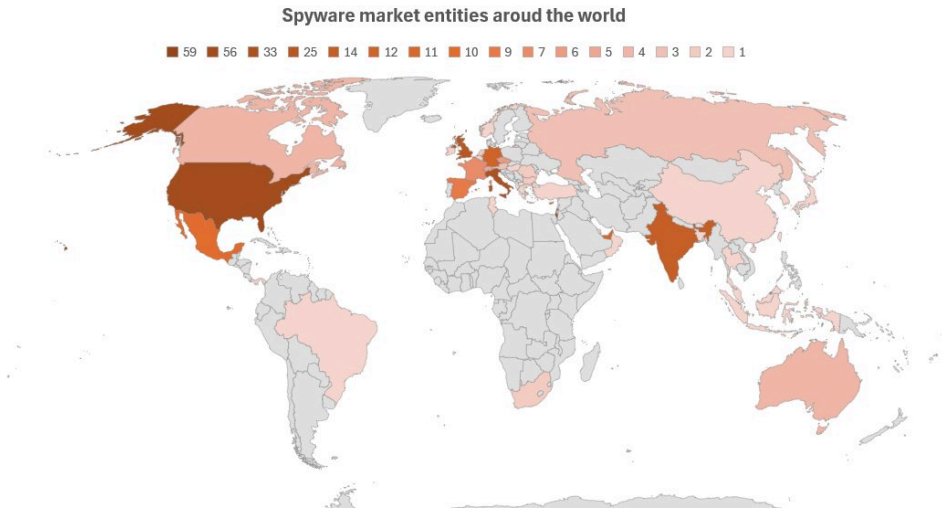


Figure 2. *Spyware market entities (subsidiaries included) around the world.* Data source: *THE STATE OF SPYWARE / A COGNITION INTELLIGENCE ANALYSIS (2026). Available at:* https:||state-of-spyware..com/. Elaboration by the author.

The main representatives of the sector, the governments of the EU, Israel and the United States, should enhance their cooperation to prevent the intrusion of digital systems from being sold to well-known human rights offenders and implement mandatory transparency controls (Feldstein et al., 2023). In particular, given that Israel is the main spyware manufacturer and exporter globally, its Ministry of Defence should be more attentive towards both the domestic enforcement of its national security and the democratic track records of recipient governments. But, as stated by cybersecurity expert Eva Galperin to The New Yorker: *"They keep expecting that the Israeli government will crack down on NSO for this [controversy], whereas, in fact, they're doing the Israeli government's bidding."* (Farrow, 2022).

The European Union, despite its relatively rigorous rules on spyware outflow and trade already in force, remains a favourable environment for the development of these kinds of technologies (Feldstein et al., 2023). Nonetheless, not even its members are safe from them. On July 3, 2026, the Citizen Lab stated that Stelios Kouloglou, a member of the PEGA Committee, reported having his devices infected with Pegasus while actively researching said malware and its implications (Scott-Railton et al., 2026). Five days later, on July 8, 2026, the European Parliament held an emergency session following the formal request by the LEFT and the Greens/EFA groups (Athens Times Newsroom, 2026). In a prior declaration, Dunja Mijatović, Commissioner for Human Rights of the Council of Europe until 2024, affirmed how it is *"virtually unimaginable that the use of Pegasus or equivalent spyware could ever be considered in accordance with the law and the necessary safeguards as outlined by the European Court of Human Rights."* (Mijatović, 2023).

A Foregone Conclusion

The NSO Group case forces a conclusion that most policy analyses tend to resist: accountability, as currently intended and practised, does not constrain commercial spyware. It legitimises it. The industry is now estimated to be worth approximately twelve billion dollars per year (Hiebert, 2023), and every judicial verdict ultimately establishes a price. Every regulatory blacklist ultimately confers the status of a newsworthy geopolitical actor. Every parliamentary committee investigation, including the one whose members were directly surveilled with the very tool under scrutiny, demonstrates that the technology is powerful enough to compromise the institutions designed to govern it. Ultimately, every academic report, including this one, contributes to envisioning Pegasus as an object of study and strategic analysis rather than a dangerous tool to be abolished.

The question, then, is not whether NSO Group will survive its legal battles, its lobbying campaigns, or its contested strategic status. It inevitably will. The question is whether liberal democracies are willing to acknowledge what the evidence already suggests: they have collectively created a market that is intrinsically incompatible with the rule of law, and the framework deployed to govern it serves primarily to manage appearances rather than actual behaviour.

Omri Lavie, NSO co-founder, clearly said that what his company does is "essential both for the State of Israel and for the world", and he may be right. However, if such technology already has the power to resist any formalised obstacle placed before it, demanding better regulation is not a conclusion; it is a way of avoiding one. It is that we have already decided, through inaction and selective enforcement, that some tools are above the law. The NSO Group did not reach that conclusion. We did.

References

Albanese, F. (2025). *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). United Nations Human Rights Council. https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/sessions-regular/session59/advance-version/a-hrc-59-23-aev.pdf

Amnesty International. (2021, July 18). *Forensic methodology report: How to catch NSO Group's Pegasus*. https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

Athens Times Newsroom. (2026, July 6). Stelios Kouloglou: Emergency debate at European Parliament over surveillance allegations. *Athens Times*. https://athens-times.com/stelios-kouloglou-emergency-debate-at-european-parliament-over-surveillance-allegations/

Blessing, J. (2024, January 26). A notorious Israeli spyware firm wants to use the Gaza war to make a comeback. *The Hill*. https://thehill.com/opinion/cybersecurity/4433419-a-notorious-israeli-spyware-firm-wants-to-use-the-gaza-war-to-make-a-comeback/

Cohen, M. S., & Freilich, C. D. (2024). *Israel: The making of a global cyber power* (Mideast Security and Policy Studies No. 209). Begin-Sadat Center for Strategic Studies, Bar-Ilan University. https://besacenter.org/wp-content/uploads/2024/10/MSPS209web.pdf

Davies, H., & Kirchgaessner, S. (2024, July 25). Israel tried to frustrate US lawsuit over Pegasus spyware, leak suggests. *The Guardian*. https://www.theguardian.com/news/article/2024/jul/25/israel-tried-to-frustrate-us-lawsuit-over-pegasus-spyware-leak-suggests

De Martin, E. (2024). *From shadows to spotlight: Analyzing NSO Group's cyber-surveillance legitimation practices in Israel* [Master's thesis, Charles University]. Charles University Digital Repository. https://dspace.cuni.cz/bitstream/handle/20.500.11956/197690/120483612.pdf?sequence=1

Dennett, L. (2018, February 21). *Closing the loophole on foreign influence*. Project On Government Oversight. https://www.pogo.org/analyses/closing-loophole-on-foreign-influence

Farrow, R. (2022, April 18). How democracies spy on their citizens. *The New Yorker*. https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens

Feldstein, S., & Kot, B. (2023, March 14). *Why does the global spyware industry continue to thrive? Trends, explanations, and responses*. Carnegie Endowment for International Peace. https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf

Frenkel, A. (2024, December 24). *Omri Lavie: Rare interview on the storms surrounding Pegasus and NSO* [Video]. YouTube. https://www.youtube.com/watch?v=yqfoL2ZDI04

Ganon, T. (2022, February 7). No one was immune: Israel Police Pegasus surveillance list revealed. *CTech*. https://www.calcalistech.com/ctech/articles/0,7340,L-3928830,00.html

Gray, C. H. (2025). *AI, sacred violence, and war: The case of Gaza*. Palgrave Macmillan. https://library.oapen.org/bitstream/handle/20.500.12657/98583/9783031815010.pdf

Harwell, D., Nakashima, E., & Timberg, C. (2021, November 3). Biden administration blacklists NSO Group over Pegasus spyware. *The Washington Post*. https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/

Hiebert, K. V. (2023, March 27). *The growing global spyware industry must be reined in*. Centre for International Governance Innovation. https://www.cigionline.org/articles/the-growing-global-spyware-industry-must-be-reined-in/

Ilnai, I. (2025, April 4). How the US led to Israel's offensive cyber collapse. *Israel Hayom*. https://www.israelhayom.com/2025/04/04/how-the-us-led-to-israels-offensive-cyber-collapse/

Lieber, D. (2025, March 12). Israeli spyware maker NSO gets new owners, leadership and seeks to mend reputation. *The Wall Street Journal*. https://www.wsj.com/tech/israeli-spyware-maker-nso-gets-new-owners-leadership-and-seeks-to-mend-reputation-166ac50e

Lobbying registration: NSO Group [Lobbying Disclosure Act filing]. (n.d.). U.S. House of Representatives, Lobbying Disclosure Act Database. https://lda.gov/filings/public/filing/9447bf56-aefd-4570-b574-d0d42a81b032/print/

Lubin, A. (2024). Selling surveillance. *Ohio State Law Journal*, *85*(5), 809–893. https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=4136&context=facpub

Mijatović, D. (2023, January 27). *Highly intrusive spyware threatens the essence of human rights*. Council of Europe, Commissioner for Human Rights. https://www.coe.int/en/web/commissioner/-/highly-intrusive-spyware-threatens-the-essence-of-human-rights

Mitra, D. (2026, June 10). Meta says NSO continued Pegasus operations despite WhatsApp injunction, seeks contempt ruling. *The Wire*. https://thewire.in/tech/meta-says-nso-continued-pegasus-operations-despite-whatsapp-injunction-seeks-contempt-ruling

Novo, L. (2025). *Spyware blasts: Strict liability for abnormally dangerous activities*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2025/09/Spyware-blasts.pdf

Panagiotopoulos, V. (2026, March 4). Will NSO's US lobbying pay off under Trump? *Tech Policy Press*. https://www.techpolicy.press/will-nsos-us-lobbying-pay-off-under-trump/

Rubin, S. (2022, January 18). Israeli police accused of using Pegasus spyware on domestic opponents of Netanyahu. *The Washington Post*. https://www.washingtonpost.com/world/2022/01/18/israel-pegasus-activists-spyware/

Scott-Railton, J., Marczak, B., Abdul Razzak, B., Pundyk, K., Anstis, S., & Deibert, R. (2026, July 3). *Espionage against the European Parliament: Member of Committee Investigating Spyware hacked with Pegasus* (Citizen Lab Report No. 194). University of Toronto, The Citizen Lab. https://citizenlab.ca/research/member-of-committee-investigating-spyware-hacked-with-pegasus/

Silberman, M. (2024). Policing Pegasus: The promise of U.S. litigation for commercial spyware accountability. *Georgetown Law Technology Review*, *8*(1), 245–286. https://georgetownlawtechreview.org/policing-pegasus-the-promise-of-u-s-litigation-for-commercial-spyware-accountability/GLTR-01-2024/

Simons, M. (2024, November 7). Judge weighs sanctions against Israeli spyware company NSO Technologies. *Courthouse News Service*. https://www.courthousenews.com/judge-weighs-sanctions-against-israeli-spyware-company-nso-technologies/

Trump, D. J. (2016, December 15). *President-elect Donald J. Trump nominates David Friedman as U.S. ambassador to Israel* [Press release]. The American Presidency Project. https://www.presidency.ucsb.edu/documents/press-release-president-elect-donald-j-trump-nominates-david-friedman-us-ambassador-israel

U.S. Department of Commerce. (2021, November 3). *Commerce adds NSO Group and other foreign companies to Entity List for malicious cyber activities* [Press release]. https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list

Ward, A. (2023, January 11). Why Israel won't change course on Ukraine. *POLITICO*. https://www.politico.com/newsletters/national-security-daily/2023/01/11/why-israel-wont-change-course-on-ukraine-00077408