Litigating Commercial Spyware:

The Promise and Limits of Private Enforcement in a New Age of Cybersurveillance

Yotam Berger*

29 STAN. TECH. L. REV. 152 (2026)

ABSTRACT

Commercial spyware firms—private companies that develop and sell sophisticated hacking tools to governments—are operating in a legal environment marked by weak oversight and notable regulatory gaps. NSO Group, the Israeli company behind the Pegasus spyware, offers a prominent example. Although marketed as a lawful investigative tool, Pegasus has also been used to target journalists and political opposition, prompting global concern and a wave of litigation.

This Article examines litigation against NSO in the United States and Israel as a case study to evaluate whether private lawsuits can function as a regulatory tool in this underregulated industry. Drawing on a comprehensive analysis of court dockets in the United States and Israel, as well as original interviews with attorneys involved in these proceedings, the Article supports the observation that traditional state-centered regulation has struggled to constrain commercial spyware. It further demonstrates that lawsuits brought by individual victims have faced considerable challenges, due to jurisdictional hurdles and structural resource disparities.

---

*JSD Candidate, Stanford Law School.

I would like to thank Michael Birnhack, Bruria Friedman-Feldman, Amalia Kessler, Leo You Li, Asaf Lubin, Uri Sabach, Shirin Sinnar, David Sklansky, Paul Stephan, Allen Weiner, and the Stanford Technology Law Review editorial board for their comments and guidance. This project was made possible by the support of the Stanford Interdisciplinary Graduate Fellowship, and Knight-Hennessy Scholars, for which I am grateful. Opinions and any mistakes are, of course, my own.

At the same time, litigation initiated by major technology companies has achieved limited success and could occupy an effective supplemental regulatory role. Building on the emerging scholarship painting Big Tech as a potential de facto complementary regulator in the field of surveillance in general, and in the context of spyware in particular, this Article shows that technology companies possess incentives, resources, and jurisdictional leverage necessary to pursue or back sustained litigation aimed at shaping legal rules that alter the economic and legal viability of abusive spyware use.

TABLE OF CONTENTS

INTRODUCTION

Francesco Corallo, an Italian-Dutch businessman and casino owner,[1] has little in common with Carlos Dada, co-founder of El Faro, an independent news outlet in El Salvador,[2] or with Elatr Khashoggi, the widow of murdered Saudi journalist Jamal Khashoggi.[3] These individuals come from remarkably different backgrounds and have led very different lives, yet they share one defining experience: each has allegedly been targeted by NSO Group's Pegasus spyware, and later attempted to hold NSO accountable through litigation in U.S. courts.

The fact that each of these individuals had to litigate against NSO in the United States, despite not being targeted by NSO on American soil, is the product of a broader regulatory crisis. Indeed, as the literature has observed, the rise of commercial spyware firms—private companies that develop and sell sophisticated hacking tools to governments worldwide[4]—has challenged existing legal and regulatory frameworks on both domestic and international levels.[5] These firms market their products as essential tools for law enforcement and national security, yet the technology is frequently abused. Neither domestic regulations nor international norms have provided meaningful constraints on their operations.

This Article examines litigation against commercial spyware, using NSO Group as a case study, and explores the potential role of such litigation as a

---

[1] *Corallo claims his phone was hacked on orders of Italy and the Netherlands*, THE DAILY HERALD (Jan. 18, 2022), www.thedailyherald.sx/islands/corallo-claims-his-phone-was-hacked-on-orders-of-italy-and-the-netherlands [https://perma.cc/2J5U-CRM5].

[2] *Carlos Dada*, INTERNATIONAL CENTER FOR JOURNALISTS, www.icfj.org/about/profiles/carlos-dada [https://perma.cc/34N9-W6TW] (last visited Dec. 15, 2025).

[3] Alex Hannaford, *'He couldn't see light at the end of the tunnel': Jamal Khashoggi's widow on their life and his death*, THE GUARDIAN (Feb. 10, 2024), www.theguardian.com/world/2024/feb/10/he-couldnt-see-light-at-the-end-of-the-tunnel-jamal-khashoggi-widow-on-their-life-and-his-death [https://perma.cc/PWZ3-F848].

[4] Asaf Lubin, *Selling Surveillance,* 85 OHIO ST. L.J. 809, 816 (2024).

[5] Natalie R. Davidson, *Big Tech as Transnational Spyware Regulator*, 36 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 477, 480-81 (2026).

complementary regulatory mechanism in an industry where traditional oversight has proven ineffective. It presents three primary observations.

First, domestic regulatory frameworks are ill-equipped to prevent the abuse of commercial spyware.

Second, individuals targeted by spyware have pursued litigation, which could have helped, at least in part, fill this gap. However, these lawsuits have encountered jurisdictional and structural obstacles. U.S. courts have generally declined to hear such cases, pointing instead to Israel as the more appropriate forum. Yet, as this Article demonstrates through interviews with attorneys involved in Israeli litigation, legal proceedings there remain secretive and have thus far also failed to provide meaningful redress.

Third, where traditional regulatory mechanisms and individual lawsuits fail, tech giants are positioned to act as de facto regulators, especially through U.S. litigation. Based on docket analysis and drawing on the emerging body of literature examining Big Tech's regulatory role as a surveillance intermediary generally, and in the spyware context in particular,[6] the Article highlights the opportunity arising from this form of litigation. The Article warns, however, that this arrangement is fragile, and that courts should be aware of its fragility when deciding these cases.

Section I provides essential background on the commercial spyware industry. It defines commercial spyware before turning to NSO Group as a case study. It examines NSO's operations, the regulatory frameworks governing its activities, and the sanctions imposed on the company by the United States in response to its spyware's alleged misuse.

Section II analyzes litigation against NSO in the United States and Israel. It first reviews lawsuits initiated by individuals in American courts and points out that these courts have identified Israel as the appropriate forum. It then examines litigation in Israel, concluding that structural limitations have made litigation there ineffective. The section then examines lawsuits brought by technology companies in U.S. courts, with particular focus on *WhatsApp v. NSO*,

---

[6] *Id.*; Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 122-44 (2018).

in which a district court found NSO liable, only to later grant the defendant's motion for remittitur.[7]

Section III identifies the inherent limitations of existing administrative regulatory frameworks relevant to the commercial spyware industry. It identifies the primary challenges that prevent state agencies from effectively mitigating the harms posed by commercial spyware. The section then argues that tech giants are equipped to step in through this form of private enforcement. Drawing on the concept of tech firms as "surveillance intermediaries,"[8] it explores how this potential quasi-regulatory role aligns with their broader incentives.

Ultimately, this Article contends that litigation may serve as a potential complementary mechanism for regulating commercial spyware. As courts reject claims brought by individual plaintiffs and regulatory agencies struggle to keep pace with rapidly evolving surveillance technologies, the role of private enforcement in shaping the future of privacy demands greater attention. If traditional regulatory institutions struggle to mitigate the abuses of the commercial spyware industry, private actors may step in to fill the void.

I. COMMERCIAL SPYWARE

A. A Hidden Industry

Commercial spyware firms develop and sell sophisticated hacking tools, often to government clients, and present themselves as providers of law enforcement and national security solutions.[9] These products raise novel legal questions regarding the appropriate mechanisms for regulating them and their cross-border trade. Sometimes, these products take advantage of zero-day

---

[7] Order re Mot. for Summ. J., WhatsApp Inc. v. NSO Group Technologies Ltd., No. 4:19-cv-07123 (N.D. Cal. Dec. 20, 2024).

[8] Rozenshtein, *supra* note 6.

[9] *E.g.*, NICOLE PERLROTH, THIS IS HOW THEY TELL ME THE WORLD ENDS 177-79 (2021); Caitlin Chin-Rothmann, *Cyber Mercenaries: Limiting Government Use of Commercial Spyware*, GEO. J. OF INT'L AFF. ONLINE (Sep. 4, 2024), https://gjia.georgetown.edu/business-economics/cyber-mercenaries-limiting-government-use-of-commercial-spyware [https://perma.cc/R8HN-WWDA].

vulnerabilities: flaws in software that can be exploited by third parties and are unknown to the software manufacturer and the public.[10] Over the past few decades,[11] a market has developed around the discovery and trade of these vulnerabilities, allowing hackers capable of identifying such exploits to sell their findings for profit.[12] Vulnerabilities that are both zero-day *and* zero-click, meaning they do not even need the targets to click a malicious link for their devices to be compromised, can be especially valuable when exploited.[13]

A zero-day vulnerability is, at its core, information—a discovery of a flaw in a program that one could exploit, defend against, or patch.[14] Over approximately the past 15 years, a market has emerged that builds upon these vulnerabilities: the commercial spyware market.[15] This industry is composed of private companies that not only identify and disclose vulnerabilities but also develop and sell the tools necessary to exploit them.[16] In essence, it is a market that offers vulnerability exploitation as a service.

Most prominently, this market has developed as a setting in which private hacking firms provide software to state actors, enabling them to infiltrate digital devices for surveillance purposes.[17] Governments across the world, both democratic and not, have entered into contracts with commercial spyware firms

---

[10] *See* Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 406, 408 (2015) (zero-day vulnerabilities are not to be confused with zero click vulnerabilities, meaning vulnerabilities that could get exploited without the need for the target user to click a malicious link, etc.); *see also* Mailyn Fidler, *Zero Progress on Zero-Days: How the Last Ten Years Created the Modern Spyware Market*, 102 NEB. L. REV. 713, 720-21 (2023) (discussing the changes the zero-day market has undergone).

[11] Fidler, *Regulating the Zero-Day Vulnerability Trade*, *supra* note 10, at 413.

[12] PERLROTH, *supra* note 9, at 41.

[13] *E.g.*, *BLASTPASS: NSO Group iPhone Zero-Click, Zero-Day Exploit Captured in the Wild*, THE CITIZEN LAB (Sep. 7, 2023), www.citizenlab.ca/2023/09/blastpass-nso-group-iphone-zero-click-zero-day-exploit-captured-in-the-wild [https://perma.cc/EHA4-E77Z].

[14] LILLIAN ABLON & ANDY BOGART, ZERO DAYS, THOUSANDS OF NIGHTS iii (2017).

[15] Steven Feldstein & Brian Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*, 1, 15 (Carnegie Endowment for Int'l Peace, Working Paper, 2023), https://assets.carnegieendowment.org/static/files/Feldstein_Global_Spyware.pdf [https://perma.cc/7CK6-WPYF].

[16] Jen Roberts et al., Mythical Beasts and Where to Find Them: Mapping the Global Spyware Market and Its Threats to National Security and Human Rights 2 (2024).

[17] *E.g.*, *id.* at 1; Fidler, *Zero Progress*, *supra* note 10.

to gain access to such tools, integrating them into law enforcement, intelligence, and national security operations.[18] Yet while these tools are often justified on the grounds of legitimate interests, their proliferation has raised significant concerns regarding their potential abuse, particularly in suppressing dissent or targeting political opposition.

Naturally, this industry operates largely in the shadows. However, information about its business leaks occasionally.[19] According to publicly available information, as Fidler observes, this market has shifted in several respects over the last decade, notably from a market in which "independent" vulnerability sellers are prominent, to one in which "full-service spyware companies . . . have become more central."[20]

In this regard, NSO Group is likely the most infamous commercial spyware vendor, and its Pegasus spyware has attracted unusually sustained public, scholarly, and legal attention.[21] NSO Group is therefore an appealing case study, in part because relatively comprehensive information about the company, its products, its clients, and the litigation against it is publicly available. At the same time, however, NSO Group is in many respects the "white whale" of the commercial spyware industry: it has become the industry's symbol, and precisely because of that symbolic status, it has attracted a degree of scrutiny—and, likely, litigation—that other spyware vendors have not faced.

It is therefore important to bear in mind that any conclusions this Article draws about the efficacy of litigation in the commercial spyware space, based on the case study examined here, are necessarily subject to limitations. Litigation against other spyware companies, including firms that have not become publicly prominent symbols of the industry, may well prove even more difficult. Those firms may operate with less public visibility, attract less sustained media and civil society attention, generate fewer publicly available records, and

---

[18] Feldstein & Kot, *supra* note 15.

[19] *E.g.*, *id.* at 8.

[20] Fidler, *Zero Progress*, *supra* note 10, at 720-21.

[21] *E.g.*, *Pegasus Project*, Forbidden Stories, www.forbiddenstories.org/projects_posts/pegasus-project/ [https://perma.cc/US83-8HFJ] (last visited May 11, 2026).

present fewer opportunities for plaintiffs to build the factual narratives necessary to sustain complex private enforcement actions. Accordingly, NSO Group offers a valuable and unusually information-rich case study, but it should not be mistaken for a fully representative example of the commercial spyware industry as a whole.

This is important because NSO Group is far from the only actor in this market.[22] Previous research has identified dozens, and in some cases even hundreds, of entities engaged in this field, with some reports naming three jurisdictions emerging as primary hubs for commercial spyware development: Israel, India, and Italy.[23] Of the seventy-four governments found by researchers to have acquired commercial spyware products or services, fifty-six reportedly purchased from Israeli companies.[24] The spyware produced by Israeli firms extends well beyond NSO's Pegasus. For example, Paragon has recently gained prominence as a growing player in the industry, and its spyware, Graphite, has reportedly been obtained by ICE.[25]

In this regard, it is of importance to note that the use of spyware by autocratic regimes has indeed gained public and legal attention,[26] but many

---

[22] Feldstein & Kot, *supra* note 15, at 9; other reports claimed at least 80 countries have acquired commercial spyware, *see* Alexander Martin, *More than 80 countries have purchased spyware, British cyber agency warns*, THE RECORD (Apr. 19, 2023), www.therecord.media/spyware-purchased-by-eighty-countries-gchq-warns [https://perma.cc/8BLP-W3SD].

[23] ROBERTS ET AL., *supra* note 16, at 10-11.

[24] Feldstein & Kot, *supra* note 15, at 2. This report counts firms such as Cellebrite, though their product has often been described not as spyware but rather as a digital forensic tool, which poses much more moderate risks to privacy. *See*, *e.g.*, Sophie Shulman, *Cellebrite CEO: "Relocation is the biggest threat to Israeli high-tech"*, CALCALIST (Jan. 28, 2025) (Isr.), www.calcalist.co.il/market/article/s1uwlhb00ke [https://perma.cc/FH7B-PGZG]; ORIN KERR, THE DIGITAL FOURTH AMENDMENT 32 (2025).

[25] *E.g.*, A. J. Vicens, *Israeli spyware firm Paragon acquired by US investment group, report says*, REUTERS (Dec. 16, 2024) www.reuters.com/markets/deals/israeli-spyware-firm-paragon-acquired-by-us-investment-group-report-says-2024-12-16; Stephanie Kirchgaessner, *ICE obtains access to Israeli-made spyware that can hack phones and encrypted apps*, THE GUARDIAN (Sep. 2, 2025), www.theguardian.com/us-news/2025/sep/02/trump-immigration-ice-israeli-spyware [https://perma.cc/4YSK-B56N].

[26] *E.g.*, Haroon Siddique & Stephanie Kirchgaessner, *Saudi Arabia ordered to pay £3m to London dissident over Pegasus spying*, THE GUARDIAN (Jan. 26, 2026) www.theguardian.com/world/2026/jan/26/saudi-arabia-ordered-pay-london-dissident-pegasus-spying-ghanem-al-masarir [https://perma.cc/6RDY-PQYM].

democratic countries have been identified as clients of spyware firms as well.[27] Within the European Union, at least fourteen of the twenty-seven member states have purchased spyware.[28] A report by an investigative committee reporting to the European Parliament later found that some of these governments had misused spyware or deployed it without the necessary legal frameworks to ensure proper oversight and safeguards.[29] Similarly, in Israel, a special Ministry of Justice committee concluded that commercial spyware had been used by the police without adequate legal protections.[30] These findings suggest that the risk of human rights abuses, suppression of privacy or violations of due process potentially associated with commercial spyware are not confined to authoritarian regimes but extend to democratic countries as well, particularly where legal oversight mechanisms are inadequate or ineffective.[31]

The United States has thus far adopted a dual approach to the commercial spyware industry. On one hand, the United States has taken an aggressive stance against certain international spyware firms, viewing them as a threat to national security.[32] These efforts include the government's move to sanction

---

[27] ROBERTS ET AL., *supra* note 16.

[28] Omer Benjakob, *Pegasus Spyware Maker NSO Has 22 Clients in the European Union. And It's Not Alone,* HAARETZ (Aug. 9, 2022), www.haaretz.com/israel-news/security-aviation/2022-08-09/ty-article/.premium/israeli-spyware-maker-nso-has-22-customers-in-12-eu-countries-and-its-not-alone/00000182-8403-df1d-a3a7-ae9bce800000 [https://perma.cc/ER7L-KK3X].

[29] *REPORT of the investigation of alleged contraventions and maladministration in the application of Union law in relation to the use of Pegasus and equivalent surveillance spyware*, (May 22, 2023), www.europarl.europa.eu/doceo/document/A-9-2023-0189_EN.html [https://perma.cc/424E-36ZU].

[30] AMIT MERARI, ZAFRIR KATZ & EYAL DAGAN, FINDINGS OF THE REVIEW TEAM REGARDING WIRETAPPING THROUGH COMPUTER COMMUNICATION IN RELATION TO THE PUBLICATION IN CALCALIST (2022) (Isr.), www.gov.il/BlobFolder/news/01-report-merari/he/Report-merari.pdf [https://perma.cc/4QUU-KFVV].

[31] Yotam Berger, The Pegasus Era: Regulating a New Generation of Government Malware, 56 GEO. J. INT'L L. 553, 553 (2025).

[32] David Klepper, US imposes sanctions on a spyware firm behind a tool used to spy on dissidents and journalists, ASSOCIATED PRESS (Sep. 16, 2024), www.apnews.com/article/spyware-sanctions-intellexa-israel-biden-treasury-3951466b68fd592f4db4e164525de824 [https://perma.cc/YQA9-93WL].

several spyware companies, along with associated individuals.[33] On the other hand, the United States has itself been a consumer of commercial spyware for law enforcement purposes. The U.S. government gained access to NSO Group's Pegasus, presumably for "testing and evaluation,"[34] before the firm was later blacklisted by the U.S. Department of Commerce.[35] More recently, U.S. law enforcement agencies have reportedly acquired Graphite.[36] In fact, public reports suggest that Paragon has tailored its business strategy to align with U.S. law and interests.[37]

B. NSO Group's Pegasus as a Case Study

NSO Group is arguably the most well-known commercial spyware firm. It gained attention first and foremost due to the extensive coverage of its operations, particularly following the Pegasus Project, an investigative effort led by the French publication Forbidden Stories in 2021.[38] The company, though, had existed and attracted scrutiny well before that. Founded around 2010 by

---

[33] E.g., Press Release, U.S. Dep't of Commerce, Treasury Sanctions Members of the Intellexa Commercial Spyware Consortium, (Mar. 5, 2024), https://home.treasury.gov/news/press-releases/jy2155 [https://perma.cc/3AC3-WB92].

[34] Mark Mazzetti & Ronen Bergman, Internal Documents Show How Close the F.B.I. Came to Deploying Spyware, N.Y. TIMES (Nov. 15, 2022), www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html.

[35] Press Release, US Dep't of Commerce, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities, (Nov. 3, 2021), www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [https://perma.cc/4QN6-7L2F].

[36] Mark Mazzetti & Ronen Bergman, Lawmakers Signal Inquiries Into U.S. Government's Use of Foreign Spyware, N.Y. TIMES (Dec. 28, 2022), www.nytimes.com/2022/12/28/us/politics/spyware-israel-dea-fbi.html.

37 Thomas Brewster, Meet Paragon: An American-Funded, Super-Secretive Israeli Surveillance Startup That 'Hacks WhatsApp And Signal', Forbes (July 29, 2021), 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/ [https://perma.cc/DW3J-F44T]; Mehul Srivastava & Kaye Wiggins, Cyberweapon manufacturers plot to stay on the right side of US, Financial Times (May 31, 2023), www.ft.com/content/11cb394d-a13e-4826-b580-823b9367fedb; Mark Mazzetti, Ronen Bergman, & Matina Stevis-Gridneff, *How the Global Spyware Industry Spiraled Out of Control*, N.Y. TIMES (Dec. 8, 2022), www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html.

[38] Pegasus Project, *supra* note 21.

three Israeli entrepreneurs,[39] NSO Group developed Pegasus, a spyware that enables operators to remotely infiltrate mobile devices.[40] To this day, NSO Group's official website presents the company as "developing technology to prevent and investigate terror and crime."[41]

In this regard, NSO Group is an appealing case study because there is a relatively substantial amount of publicly-available information concerning its product and the legal challenges brought against it. At the same time, however, NSO's public prominence is not representative of most actors in the commercial spyware industry. That distinction imposes meaningful limits on what can be inferred "as is" from the NSO litigation about the potential efficacy of litigation against other vendors in this field. The litigation against NSO appears to have been facilitated, at least in part, by the extensive media coverage, civil society attention, and public scrutiny that the company has attracted. One possible implication, then, is that some of the insights drawn from this case study may travel more broadly only where litigation is accompanied by, or is the result of, sustained public attention and civil society action.[42]

NSO, then, reportedly originated in a company named CommuniTake, which developed a product allowing support technicians to remotely access customers' phones.[43] The company's founders soon realized the technology could be repurposed to gather intelligence.[44] NSO was not the first major player in the field of commercial spyware, but its technological assets drew significant attention even before the Pegasus Project. For instance, reports emerged that, around 2017, NSO's spyware had been used to target supporters of a tax reform initiative in Mexico aimed at imposing a soda tax to curb the consumption of

---

[39] Gabrielle Coppola, *Israeli Entrepreneurs Play Both Sides of the Cyber Wars*, BLOOMBERG (Sep. 29, 2014), www.bloomberg.com/news/articles/2014-09-29/israeli-entrepreneurs-play-both-sides-of-the-cyber-wars.

[40] *E.g.*, David Pegg & Sam Cutler, *What is Pegasus spyware and how does it hack phones?*, THE GUARDIAN (July 18, 2021), www.theguardian.com/news/2021/jul/18/what-is-pegasus-spyware-and-how-does-it-hack-phones [https://perma.cc/8B3L-WLAJ].

[41] *About Us*, NSO GROUP, www.nsogroup.com/about-us/ (last visited Feb. 25, 2026).

[42] *E.g.*, Fidler, *Zero Progress*, *supra* note 10, at 757 (discussing the importance of investigative journalism in this context).

[43] LAURENT RICHARD & SANDRINE RIGUAD, PEGASUS 52 (2023).

[44] *Id.* at 52-55.

sugary drinks.[45] The company also faced intense scrutiny following the assassination of Jamal Khashoggi, a Saudi journalist and dissident murdered in Istanbul. Reports suggested that Pegasus had been used by the Saudi regime to surveil Khashoggi, as well as his associates and family members, prior to his killing.[46]

Although NSO is a private firm, it was later reported that the Israeli government had leveraged the company's technology for diplomatic purposes,[47] particularly given its authority to regulate the export of surveillance tools abroad.[48] For example, reports indicate that NSO's spyware played a role in negotiations between Israel and the United Arab Emirates, which later acquired the software as part of the diplomatic discussions leading to the Abraham Accords.[49] Similarly, the *New York Times* reported that countries such as Mexico and Panama shifted their voting patterns at the United Nations in favor of Israel after gaining access to Pegasus.[50]

However, NSO's global reputation crisis escalated following the publication of the Pegasus Project, a series of investigative reports exposing widespread abuses of Pegasus.[51] The central revelation was based on a leaked document, referred to as The List—a file containing approximately 50,000 phone numbers

---

[45] Nicole Perlroth, *Spyware's Odd Targets: Backers of Mexico's Soda Tax*, N.Y. TIMES (Feb. 11, 2017), www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html?module=inline.

[46] *E.g.*, David D. Kirkpatrick, *Israeli Software Helped Saudis Spy on Khashoggi, Lawsuit Says*, N.Y. TIMES (Dec. 2, 2018), www.nytimes.com/2018/12/02/world/middleeast/saudi-khashoggi-spyware-israel.html.

[47] Kali Robinson, *How Israel's Pegasus Spyware Stoked the Surveillance Debate*, COUNCIL ON FOREIGN RELATIONS (Mar. 8, 2022), https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate [https://perma.cc/Q3UB-RK9Y].

[48] Defense Export Control Law, 2007 (Isr.), www.nevo.co.il/law_html/law01/999_796.htm [https://perma.cc/GS9P-TP4X].

[49] Aluf Benn, *Netanyahu Used NSO's Pegasus for Diplomacy. Now He Blames It for His Downfall*, HAARETZ (Feb. 5, 2022), www.haaretz.com/israel-news/2022-02-05/ty-article/.premium/netanyahu-used-nsos-pegasus-for-diplomacy-now-he-blames-it-for-his-downfall/0000017f-e941-dc91-a17f-fdcd55c80000.

[50] Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. TIMES (Jan. 28, 2022), www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

[51] *Pegasus Project*, *supra* note 21; RICHARD & RIGUAD, *supra* note 43, at 1-16.

of individuals whose devices had allegedly been targeted by Pegasus.[52] The Pegasus Project featured interviews with individuals familiar with the software, who provided insight into its technical architecture.[53] Once a device was infected with Pegasus, the governmental agency operating the spyware could assume full control, gaining access to encrypted messages, real-time and historical geolocation data, and other sensitive information.[54] Moreover, operators could remotely activate the device's microphone and camera without the user's knowledge.[55]

Investigative reports and research conducted by Amnesty International and the Citizen Lab at the University of Toronto have made substantial progress in understanding how various versions of Pegasus operate.[56] Early iterations of Pegasus primarily relied on social engineering techniques rather than zero-click capabilities. For example, some versions of the software required operators to send a disguised malicious link, relying on the target to click the link in order to allow the infection.[57] As the technology evolved, more advanced versions of Pegasus no longer depended on the operator's ability to deceive the target. Instead, they exploited zero-click vulnerabilities in widely used operating systems and applications, without requiring user interaction to compromise a device.[58] These vulnerabilities reportedly affected a broad range of platforms, including Google's Android, Apple's iOS, and Meta's WhatsApp.[59]

Even after the Pegasus Project's revelations, NSO continued to insist that it sold its software exclusively as a legitimate law enforcement tool.[60] Shortly after

---

[52] *Id.*

[53] RICHARD & RIGUAD, *supra* note 43, at 81.

[54] *Pegasus Project*, *supra* note 21; RICHARD & RIGUAD, *supra* note 43, at 1-16.

[55] RICHARD & RIGUAD, *supra* note 43, at 1-16.

[56] *E.g.*, AMNESTY INTERNATIONAL, FORENSIC METHODOLOGY REPORT: HOW TO CATCH NSO GROUP'S PEGASUS (2021), www.amnesty.org/en/documents/doc10/4487/2021/en [https://perma.cc/2Y57-NKCP]; *see also* RONALD J. DEIBER, CHASING SHADOWS 111 (2025).

[57] RICHARD & RIGUAD, *supra* note 43, at 77-80, 87.

[58] *E.g.*, *BLASTPASS*, *supra* note 13.

[59] RICHARD & RIGUAD, *supra* note 43, at 79.

[60] Thomas Brewster, *'If You're Not A Criminal, Don't Be Afraid' – NSO CEO On 'Insane' Hacking*

the initial reporting by Forbidden Stories and their partners, NSO's CEO denied most of the allegations, stating that for "the people that are not criminals . . . there's nothing to be afraid of."[61] However, ongoing investigations suggested otherwise. The Washington Post reported that Pegasus had been used to target at least ten prime ministers, three presidents, and one king.[62] Other outlets have further identified dozens of journalists, civil society figures, and human rights activists who had allegedly been placed under surveillance using the spyware.[63]

Pegasus, then, was deployed by various democracies. Israel deployed the tool in the context of criminal investigations.[64] NSO had at least twenty-two client agencies across fourteen European Union member states,[65] including Germany, the Netherlands, and Spain.[66] The United States also reportedly gained access to Pegasus; the FBI purchased the software and installed its servers in a facility in New Jersey around 2019.[67] FBI Director Christopher Wray later claimed the tool had been acquired solely for research and development

---

Allegations Facing $1 Billion Spyware Business, FORBES (July 22, 2021), www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/ [https://perma.cc/38AM-4W9R]; Elizabeth Dwoskin & Shira Rubin, *'Somebody has to do the dirty work': NSO founders defend the spyware they built*, WASH. POST (July 21, 2021), www.washingtonpost.com/world/2021/07/21/shalev-hulio-nso-surveillance/.

[61] Brewster, *supra* note 60.

[62] Craig Timberg et al., *On the list: Ten prime ministers, three presidents and a king*, WASH. POST (July 20, 2021), www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.

[63] Shaun Walker et al., *Pegasus project: spyware leak suggests lawyers and activists at risk across globe*, THE GUARDIAN (July 19, 2021), www.theguardian.com/news/2021/jul/19/spyware-leak-suggests-lawyers-and-activists-at-risk-across-globe [https://perma.cc/5R24-3V9P].

[64] MERARI et al., *supra* note 30.

[65] Benjakob, *supra* note 28.

[66] Julie Fuchs, *Is the EU protecting people from Pegasus spyware?*, ACCESS NOW (Jan. 17, 2023), www.accessnow.org/eu-pegasus-spyware/ [https://perma.cc/JSL9-2DAN]; EU PEGA Report, *supra* note 29.

[67] Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. TIMES MAGAZINE (Jan. 28, 2022), www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [https://perma.cc/UG8P-Z62A].

purposes, asserting that it was never used in active investigations.[68] However, a subsequent report by *The New York Times* revealed that in late 2020 and early 2021, FBI officials had pushed to deploy Pegasus in criminal investigations.[69]

The exposure of NSO's activities and the resulting controversy severely impacted its business. One of the most immediate consequences was the withdrawal of key investors.[70] In November 2021, the United States blacklisted NSO, adding it to the Commerce Department's Entity List.[71] The U.S. government further announced visa restrictions targeting individuals involved in the abuse of surveillance technology, a move that reports have linked to the earlier sanctions imposed on NSO.[72]

NSO has continued to operate under new ownership.[73] Even after the fallout from the Pegasus Project, reports indicate that Pegasus remained in active use. In 2023, The Citizen Lab published an analysis confirming that Pegasus was still being deployed "in the wild."[74] Additionally, it was reported that the Israeli military had utilized Pegasus in its operations, specifically in

---

[68] Yonah Jeremy Bob, *FBI chief: We bought NSO's Pegasus to do counterintelligence*, THE JERUSALEM POST (Mar. 8, 2022), www.jpost.com/international/article-700689 [https://perma.cc/Z8W6-YGSF].

[69] Mark Mazzetti & Ronen Bergman, *Internal Documents Show How Close the F.B.I. Came to Deploying Spyware*, N.Y. TIMES (Nov. 12, 2022), www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html [https://perma.cc/UG8P-Z62A].

[70] Amitai Ziv, *Israeli Cyberattack Firm NSO Bought Back by Founders at $1b Company Value*, HAARETZ (Feb. 14, 2019), www.haaretz.com/israel-news/business/2019-02-14/ty-article/.premium/israeli-cyberattack-firm-nso-bought-back-by-founders-at-1b-company-value/0000017f-e16f-d75c-a7ff-fdefa46b0000 [https://perma.cc/R7VJ-BZ4S].

[71] David E. Sanger et al., *U.S. Blacklists Israeli Firm NSO Group Over Spyware*, N.Y. TIMES (Nov. 3, 2021), www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html [https://perma.cc/9GZW-YAU3].

[72] Stephanie Kirchgaessner, *US announces new restrictions to curb global spyware industry*, THE GUARDIAN (Feb. 5, 2024), www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions [https://perma.cc/8VH7-25GL].

[73] Alexander Saeedy & Dustin Volz, *Israeli Cyber Company NSO Group Has New Ownership After U.S. Blacklist*, WALL ST. J. (May 26, 2023), www.wsj.com/articles/israeli-cyber-company-nso-group-has-new-ownership-after-u-s-blacklist-a2cda00a?mod=Searchresults_pos1&page=1 [https://perma.cc/7345-97FB].

[74] Bill Marczak et al., *NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains*, THE CITIZEN LAB (Apr. 18, 2023), www.citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022.

efforts to locate Israeli hostages in Gaza.[75] In late 2025, NSO announced David Friedman, former U.S. ambassador to Israel, as its new executive chairman—part of what was framed in the press as a "bid to get off Washington's blacklist."[76] These developments hint that while NSO has faced significant challenges, their operations have persisted.

Investigative reports, leaked documents, technical analyses, and subsequent lawsuits filed against NSO have revealed a considerable amount of information about how Pegasus was operated, marketed, and deployed. These sources provide insight into both its legitimate uses and its abuses. They reveal details about NSO's clientele, the technical architecture of Pegasus, and the spyware's operational framework. Additionally, they shed light on the regulatory mechanisms that governed Pegasus at different levels and, critically, how these regulations failed to prevent its misuse.

The attention drawn to NSO Group, then, makes it an attractive case study because a comparatively large body of information about the company is publicly available. But any effort to examine NSO as a case study with the aspiration of drawing broader conclusions about the commercial spyware industry must proceed with an important caveat. The fact that NSO Group became the industry's "white whale" means that it may also have been an unusually "easy target" for litigation in a sense, or that some of the actors that pursued claims or other forms of action against it had public-relations-based incentives that do not exist, at least not to the same extent, with respect to other companies. Parts of the analysis presented here may therefore be applicable to other spyware vendors only to the extent those vendors are brought to similar public attention, or, alternatively if individuals, states, or

---

[75] Gwen Ackerman & Marissa Newman, *Israel Taps Blacklisted Pegasus Maker to Track Hostages in Gaza*, BLOOMBERG (Oct. 26, 2023), www.bloomberg.com/news/articles/2023-10-26/israel-taps-blacklisted-pegasus-maker-nso-to-track-gaza-hostages-and-hamas [https://perma.cc/GSE2-EZXW].

[76] *E.g.*, Sharon Wrobel, *Seeking to get off US blacklist, spyware firm NSO taps ex-envoy Friedman as chairman*, TIMES OF ISR. (Nov. 9, 2025), www.timesofisrael.com/seeking-to-get-off-us-blacklist-spyware-firm-nso-taps-ex-envoy-friedman-as-chairman [https://perma.cc/53D2-UNYW].

technology companies develop stronger incentives to act as regulators in this field, as they did in relation to NSO.

This means, for example, that investigative journalism, academic research, and civil society action may be especially important in the commercial spyware context because they enable public discussion that may, in turn, lead to enforcement. As Fidler observes in a related context, "nearly every major reform in this issue area came in the wake of [an] investigative report or leak. . . . Reporting on Pegasus led to an Israeli crackdown, at least temporarily, on major vendors, prompted the European Parliament's investigation, and fed into calls for a moratorium."[77] This observation may apply with particular force to the use of litigation, whether by individuals or by technology companies, as a complementary regulatory mechanism. Such litigation may become more viable, and may achieve greater regulatory significance, when it is preceded or accompanied by sustained public attention.

In other words, NSO Group illustrates what can happen when significant scrutiny is directed toward one of these vendors, and certain aspects of the analysis offered here may therefore apply primarily to entities that become subject to comparable public attention. Moreover, the importance of investigative journalism and other forms of public activity in this space extends beyond the mere exposure of information. Reporting can generate public and political discourse, which in turn, as this Article later discusses, may create or strengthen incentives for tech giants to assume a role as de facto regulators, notwithstanding contrary pressures from the spyware industry itself or from the governments that rely on it.

C. Regulating Pegasus

The regulation of commercial spyware has generally presented complex questions and persistent failures, especially—as Lubin has categorized them—when state actors, corporate governance tools, and traditional criminal and civil

---

[77] Fidler, *Zero Progress*, *supra* note 10, at 757.

enforcement mechanisms are treated as the principal avenues for regulation.[78] The "regulatory conundrum" in this space, as Davidson has observed, has resulted, among other things, in the potential emergence of technology companies as de facto regulators.[79] The scholarship in that field has pointed out before failures of the existing mechanisms, and pointed to the potentially promising role of Big Tech in this space. That scholarship identifies a range of strategies through which technology companies may influence the commercial spyware ecosystem, including, most relevant for this Article, litigation.[80]

To follow how NSO was sold to foreign regimes, and to better grasp the nuances of litigation against NSO in the United States, a brief overview of Israeli law—where NSO was regulated, and where American courts have claimed litigation against NSO is often appropriate—is in order.

Israeli law establishes a two-stage regulatory framework for Israeli entities engaged in defense exports. First, any entity seeking to engage in defense trade must obtain a general defense trade license.[81] Once such a license is secured, the entity may then apply for a specific defense export license, which is required for any transaction involving the sale of defense-related products to foreign entities.[82]

NSO obtained legal permits from DECA (Israel's Defense Export Controls Agency), and its exportation of Pegasus to foreign governments appears to have been conducted in compliance with Israeli law.[83] As previously noted, the Israeli government did not merely permit these exports, but actively supported and

---

[78] Lubin, *supra* note 4, at 816.

[79] Davidson, *supra* note 5, at 480-81.

[80] *E.g.*, *id.* at 510-15; Asaf Lubin, *Unpacking WhatsApp's Legal Triumph Over NSO Group*, LAWFARE (Jan. 7, 2025) www.lawfaremedia.org/article/unpacking-whatsapp-s-legal-triumph-over-nso-group [https://perma.cc/G3VX-CMJ8].

[81] Article 14(a), Defense Export Control Law, *supra* note 48.

[82] *Id.* art. 15.

[83] Judah Ari Gross, *Israel: If NSO Group violated export permits, 'appropriate action' will be taken*, THE TIMES OF ISRAEL (Jul. 19, 2021), www.timesofisrael.com/israel-if-nso-group-violated-export-permits-appropriate-action-will-be-taken [https://perma.cc/AC4E-SP8V].

facilitated them[84]—primarily to advance national security and diplomatic purposes.[85] Then came the Pegasus Project. The Israeli defense establishment, at least to some degree, appeared concerned by investigative reports demonstrating that its export control system had failed to prevent spyware abuse. In December 2021, the Israeli Ministry of Defense announced plans to tighten its regulatory oversight over commercial spyware.[86] By January 2022, the Ministry of Defense announced that it had revoked thousands of export licenses in response to the Pegasus scandal.[87]

The United States imposed restrictions on NSO and similar companies following revelations of Pegasus's widespread abuse. In November 2021, the Commerce Department's Bureau of Industry and Security added NSO to the Entity List, a trade restriction list that effectively bars companies from conducting business with U.S. entities.[88] In its press release, the Commerce Department cited NSO's activities as "contrary to the national security or foreign policy interests of the United States."[89] It specifically noted that Pegasus had been used to "maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers," and that such tools had "enabled foreign governments to conduct transnational repression."[90]

---

[84] Tehilla Shwartz Altshuler, פרשת NSO - סייבר, ביטחון ומה שביניהם [The NSO Affair: Cyber, Security, and Everything in Between], ISR. DEMOCRACY INST. (Jul. 20, 2021), https://www.idi.org.il/articles/36070 [https://perma.cc/9DLX-BT4G] (Isr.).

[85] Benn, *supra* note 49; Bergman & Mazzetti, *supra* note 50.

[86] Assaf Gilad, בעקבות פרשת NSO: משרד הבטחון מהדק את הסכמי ייצוא הסייבר [Following the NSO Affair: The Ministry of Defense Tightens Cyber Export Agreements], Globes (Dec. 6, 2021), www.globes.co.il/news/article.aspx?did=1001393439 [https://perma.cc/FE3F-T4NK] (Isr.).

[87] Anna Ahronheim, *Amid NSO scandal, over 3,600 export licenses revoked in the past year*, THE JERUSALEM POST (Jan. 31, 2022), www.jpost.com/israel-news/article-695084 [https://perma.cc/3A44-8GAV].

[88] Press Release, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities*, U.S. DEP'T. OF COM. (Nov. 3, 2021), www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.

[89] *Id.*

[90] *Id.*

In 2024, the United States further announced that it would impose global visa restrictions on individuals involved in the misuse of commercial spyware.[91] While the official announcement did not explicitly name NSO, it referenced sanctions against another commercial spyware firm, Intellexa.[92] However, news reports linked the policy shift to broader concerns about NSO's activities as well.[93] As noted earlier, NSO's business was harmed but not eliminated entirely following the publications by the Pegasus Project, and the company has continued to operate despite American and Israeli regulatory measures.[94]

Could Pegasus have been more effectively regulated from the outset? Scholarship has previously noted that regulatory frameworks governing defense technologies primarily consider national security concerns, often subordinating human rights considerations.[95] It has been observed that NSO Group actively sought public legitimacy, for instance by employing strategies of "patriotic legitimation" to align itself with the priorities of its regulators and the broader interests of the state.[96] Such public relations efforts make regulating spyware products more complicated. Meanwhile, international legal norms appear to have played little role in governing the export of cyber surveillance tools.[97]

This situation—the "regulatory conundrum" Davidson describes—may in turn have generated the need for private actors to act independently in seeking

---

[91] Matthew Miller, *Press Statement: Promoting Accountability for the Misuse of Commercial Spyware*, U.S. DEP'T. OF STATE (Sep. 20, 2024), www.2021-2025.state.gov/promoting-accountability-for-the-misuse-of-commercial-spyware-2.

[92] *Id.*

[93] *E.g.*, Stephanie Kirchgaessner, *US announces new restrictions to curb global spyware industry*, THE GUARDIAN (Feb. 5, 2024), www.theguardian.com/us-news/2024/feb/05/us-biden-administration-global-spyware-restrictions [https://perma.cc/ND7W-GE2F]; Omer Kabir, *Will NSO employees soon be barred from entering the US?*, CALCALIST (Feb. 7, 2024), www.calcalistech.com/ctechnews/article/b1anhnkot [https://perma.cc/43AA-XUQD].

[94] NSO Group's Webpage, *supra* note 41; Ackerman & Newman, *supra* note 75.

[95] Hilla Goldschmidt, סייבר התקפי – בין יצוא בטחוני לייבוא אביפתי [Offensive Cyber Operations – Between Security Exports and Enforcement through Importation], 41 Tel AVIV L. REV. ONLINE (2022), www.perma.cc/ZE8S-QDB5 (Isr.).

[96] Dan M. Kotliar & Elinor Carmi, *Keeping Pegasus on the Wing: Legitimizing Cyber* Espionage, 27(8) INFO., COMMC'N & SOC'Y 1499, 1505-08 (2024).

[97] Tomasz Mielko, *Could Pegasus Gate have been prevented? The evolution of the export control regime for cyber-surveillance tools in Israel*, 1(9) CYBERSECURITY AND L. 155, 158 (2023).

to restrict or constrain the commercial spyware industry.[98] This development may be understood as a specific example of a broader strategy through which Big Tech companies serve as "surveillance intermediaries," as Rozenshtein has described them.[99] That strategy has been employed by technology companies in other contexts as well, particularly where governments have sought to leverage Big Tech's capabilities, infrastructure, or data to surveil users through various means.[100] In the commercial spyware context, and especially in relation to Pegasus, Big Tech companies have employed some of these familiar techniques while also developing strategies more specific to the spyware ecosystem. These include, as Davidson points out, setting standards through the establishment of industry "accords"; leveraging political power to support measures against spyware vendors, including blacklisting relevant actors; gathering and sharing information with the public; taking concrete steps to protect targets; and engaging in standard enforcement, including through litigation.[101]

Individuals, particularly those who have themselves been targeted, have also sought to hold spyware companies to stricter legal standards. Sometimes acting alone, and other times supported by NGOs, civil society organizations, and technology companies, [102] these individuals have likewise employed strategies that include public campaigns and litigation in an effort to hold commercial spyware manufacturers accountable. The next Part examines in detail the litigation initiated by these two groups, tech giants and targeted individuals, in the United States. It then evaluates the promise and limits of these strategies as complementary mechanisms for regulating the commercial spyware industry.

---

[98] Davidson, *supra* note 5.

[99] Rozenshtein, *supra* note 6.

[100] *Id.* at 122-44.

[101] Davidson, *supra* note 5, at 502, 511-14.

[102] *E.g.*, Press Statement, *Appeals Court Revives Journalists' Case Against Spyware Manufacturer NSO Group*, KNIGHT FIRST AMEND. INST. AT COLUM. UNIV. (Jul. 8, 2025) https://knightcolumbia.org/content/appeals-court-revives-journalists-case-against-spyware-manufacturer-nso-group [https://perma.cc/RQ5Z-ZJBH] (illustrating the support of the Knight Institute in the Dada case).

II. SUING NSO

While NSO is just one company within a broader industry, it has drawn uniquely broad global attention, primarily due to the Pegasus Project's revelations. [103] This publicity has led to extensive media coverage, investigations, and litigation worldwide. A review by the Citizen Lab identified multiple jurisdictions where NSO or its clients have faced legal challenges, including the United Kingdom, Colombia, Thailand, Spain, Mexico, Hungary, Poland.[104] Cases range from civil litigation against NSO to criminal investigations into the use of Pegasus and lawsuits challenging governments accused of abusing the spyware.[105]

Litigation in the United States and Israel challenging NSO has been most prominent, especially as NSO is based in Israel and the facilities its product exploit are located in the United States.[106] These proceedings broadly fall into two categories: lawsuits brought by individuals, particularly those targeted by Pegasus or their allies, and lawsuits filed by tech giants whose platforms have been exploited by NSO's spyware. This section reviews litigation against NSO in these two jurisdictions.

A. Litigation by Individuals

By design, individuals targeted by Pegasus in an abusive manner often face significant barriers to suing NSO in their home jurisdictions, which are

---

[103] The Pegasus Project, *supra* note 21; RICHARD & RIGUAD, *supra* note 43.

[104] Siena Anstis, *Litigation and other formal complaints related to mercenary spyware*, THE CITIZEN LAB (Dec. 12, 2018), www.citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry.

[105] *Id.*

106 Id.; e.g., Michael Silberman, Policing Pegasus: The Promise of U.S. Litigation for Commercial Spyware Accountability, 8(1) Geo. L. Tech. Rev. 245 (2024); Allie Schiele, Spyware Company NSO Group Faces Setbacks in Attempts to Avoid US Lawsuits, JUST SECURITY (Jan. 17, 2025), www.justsecurity.org/106536/nso-whatsapp-lawsuit [perma.cc/J3EN-Y3UY]; Raphael Satter, Exposed Israeli spy linked to apparent effort by NSO Group to derail lawsuits, THE TIMES OF ISRAEL (Feb. 11, 2019), www.timesofisrael.com/exposed-israeli-spy-linked-to-apparent-effort-by-nso-group-to-derail-lawsuits [perma.cc/T9KT-BL7Y].

frequently authoritarian.[107] Even if the country that has abusively deployed the spyware is not authoritarian, potential plaintiffs tend to prefer litigation in jurisdictions other than the one in which the spyware was abusively used by the government. This practice, however, creates a jurisdictional challenge: plaintiffs must find a foreign court willing to assert jurisdiction even though their devices were not physically targeted within that jurisdiction. A favored forum option is the United States, where the platforms whose vulnerabilities were exploited by Pegasus operate. Another option is Israel, where NSO Group is headquartered, and where—as reviewed here—American courts have sometimes found litigation to be appropriate.

1. In the United States

At least three lawsuits have been filed in U.S. courts by individuals targeted by Pegasus: *Corallo*; *Dada*; and *Khashoggi*.

Corallo v. NSO was the first case this Article identifies in which an individual sued NSO in the United States.[108] Francesco Corallo, a native of Italy, citizen of the Netherlands, and resident of Sint Maarten in the Dutch Caribbean,[109] filed his complaint on September 13, 2022, against both NSO and Apple.[110] Corallo alleged that his iPhone, which had been backed up to iCloud, was hacked using NSO's FORCEDENTRY exploit—a vulnerability used to target Apple devices[111]—"on behalf of a governmental client."[112] Seeking remedies from both the iPhone's manufacturer and the commercial spyware firm, Corallo filed suit in the Northern District of California.[113]

---

[107] Feldstein & Kot, supra note 15, at 17.
[108] Order re Mot. to Dismiss, Corallo v. NSO Grp. Techs., No. 22-cv-05229 (N.D. Cal. Nov. 6, 2024).
[109] Compl. at 2, Corallo v. NSO Grp. Techs., No. 3:22-cv-05229 (N.D. Cal. Sept. 13, 2022).
[110] *Id.*
[111] Bill Marczak et al., *FORCEDENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild*, THE CITIZEN LAB (Sep. 13, 2021), www.citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild.
[112] *Id.*
[113] Compl. at Corallo v. NSO, *supra* note 109.

Both NSO and Apple submitted motions to dismiss. NSO brought jurisdiction and *forum non conveniens* claims, arguing that Israel was the appropriate forum for legal claims against the company.[114] Apple moved to dismiss on the grounds of failure to state a claim.[115]

On September 30, 2024, the U.S. District Court for the Northern District of California granted both motions to dismiss.[116] Regarding NSO, the court found that the company had no actual presence in the United States at the relevant time.[117] Corallo argued that although his device was not on United States soil, in order to compromise his phone, NSO had hacked into Apple's servers, which were physically located in California. The court, however, found that Corallo failed to demonstrate that NSO's conduct was "expressly aimed at California and caused harm that NSO knew likely would be suffered in California."[118] The fact that Corallo himself had neither a connection to nor a presence in California, the court noted, "undermines any argument that the conduct was targeted at California or that harm was likely to be suffered [there]."[119] Additionally, the court found that "Corallo's insistence that NSO targeted Apple's servers in California was not only speculative as a factual matter, but legally insufficient to give rise to personal jurisdiction over NSO."[120]

Interestingly, the court also determined that even if Corallo had established a jurisdictionally significant connection, NSO had made a "compelling case" that exercising jurisdiction in Northern California would be unreasonable.[121] The court emphasized that Corallo, a foreign citizen, was suing other foreign citizens for conduct that originated abroad. Consequently, dismissal was also warranted

---

[114] NSO Grp. Techs.'s Mot. to Dismiss, Corallo v. NSO Grp. Techs., No. 3:22-cv-05229 (N.D. Cal. Mar. 10, 2023).
[115] Apple Inc.'s Mot. to Dismiss, Corallo v. NSO Grp. Techs., No. 3:22-cv-05229 (N.D. Cal. Nov. 4, 2022).
[116] Order re Mot. to Dismiss, Corallo v. NSO Grp. Techs., No. 22-cv-05229 (N.D. Cal. Sep. 30, 2024).
[117] *Id.* at 5.
[118] *Id.* at 6.
[119] *Id.*
[120] *Id.*
[121] *Id.*

under the *forum non conveniens* doctrine, and Israel was deemed the more appropriate forum.[122]

Dada v. NSO initially met a similar fate,[123] though an appeal to the Ninth Circuit[124] resulted in a remand to the district court for reconsideration, noting that domestic U.S. plaintiffs were involved.[125]

On November 30, 2022—approximately two months after Corallo initiated his legal action—a group of journalists from the independent news organization El Faro, based in El Salvador, filed suit against NSO in the U.S. District Court for the Northern District of California.[126] The plaintiffs alleged that they had been targeted by Pegasus between June 2020 and November 2021 and sued NSO for violations of U.S. statutes, including the Computer Fraud and Abuse Act (CFAA),[127] the California Comprehensive Computer Data Access and Fraud Act (CDAFA),[128] as well as claims of trespass and intrusion. NSO, in response, moved to dismiss the case, once again citing lack of jurisdiction and invoking the *forum non conveniens* doctrine.[129]

On March 8, 2024, the district court granted NSO's motion and dismissed the case on *forum non conveniens* grounds.[130] The court emphasized:

"The nub of this case is entirely foreign and concerns the use of software produced in Israel to hack devices owned by a Salvadoran news service and used by journalists in El Salvador. Every incident described in the complaint involved Salvadoran journalists covering Salvadoran news stories while working primarily in El Salvador. There is little reason under the forum non conveniens factors to undertake the burden of litigating this foreign conduct here. NSO states, and

---

[122] *Id.* at 7.
[123] Order re Mot. to Dismiss, Dada v. NSO Grp. Techs., No. 3:22-cv-07513 (N.D. Cal. Mar. 8, 2024).
[124] Dada v. NSO Grp. Techs., No. 24-2179, (9th Cir.)
[125] Dada v. NSO Grp. Techs., No. 24-2179, (9th Cir. Jul. 8, 2025).
[126] Compl., Dada v. NSO Grp. Techs., No. 3:22-cv-07513 (N.D. Cal. Nov. 30, 2022).
[127] 18 U.S.C. § 1030.
[128] Cal. Penal Code § 502.
[129] NSO Grp. Techs.'s Mot. to Dismiss, Dada v. NSO Grp. Techs., No. 3:22-cv-07513 (N.D. Cal. Apr. 20, 2023).
[130] Order re Mot. to Dismiss, Dada v. NSO, *supra* note 123.

plaintiffs do not dispute, that Israel is an adequate alternative forum. This is all the more true because NSO expressly states that 'as a citizen of Israel, NSO is amenable to process in Israel.'"[131]

On April 8, 2024, the plaintiffs filed a notice of appeal to the Ninth Circuit, contesting the district court's decision.[132] The appeal has received notable support from several amicus briefs, including one submitted on July 22, 2024, by a coalition of major technology companies, including .Microsoft, Google, and GitHub[133] The amici assert that the district court failed to adequately consider the national security implications of allowing such litigation to proceed in the United States rather than deferring to a foreign jurisdiction.[134] Additionally, the brief underscores the United States' and California's vested interest in protecting domestic technology firms.[135]

On July 8, 2025, the Ninth Circuit remanded the case, finding that the district court had abused its discretion by misapplying the forum non conveniens doctrine.[136] In its decision, the majority emphasized that two of the plaintiffs in *Dada* are U.S. residents, and one is a U.S. citizen. The court found that the district court "abused its discretion by failing to recognize that it should apply an intermediate level of deference under such circumstances" and instead described the standard applicable to purely foreign plaintiffs.[137] A dissenting opinion suggested that the district court properly declined to assert jurisdiction.[138]

The third case filed by an individual and litigated in the United States is *Khashoggi v. NSO*,[139] brought by Elatr Khashoggi, the widow of the late Jamal

---

[131] *Id.* at 4-5.
[132] Dada v. NSO Grp. Techs., 24-2179 (9th Cir.).
[133] Brief for Microsoft, Google, GitHub et al. as Amici Curiae, Dada v. NSO Grp. Techs., 24-2179 (9th Cir.).
[134] *Id.* at 13.
[135] *Id.* at 28.
[136] Order to Remand, Dada v. NSO Grp. Techs., 24-2179 (9th Cir.).
[137] *Id.* at 3-4.
[138] *Id.* at 6-9.
[139] Order re Mot. to Dismiss, Khashoggi v. NSO Grp. Techs., No. 1:23-cv-00779 (E.D. Va. Oct. 26, 2023).

Khashoggi.[140] In the complaint, she has claimed that both she and Jamal were residents of Virginia,[141] and that Jamal was reportedly targeted using Pegasus by Saudi Arabia prior to his assassination.[142] His widow, Elatr, was also reportedly targeted by the spyware.[143] Her lawsuit alleged that she had been targeted by Pegasus and that information obtained from her phone was later used to facilitate the surveillance and assassination of her husband.[144] The complaint was filed on June 15, 2023 in the Eastern District of Virginia, asserting various causes of action, including violations of the Computer Fraud and Abuse Act (CFAA)[145] and the Virginia Computer Crimes Act.[146] NSO filed a motion to dismiss, arguing lack of jurisdiction and failure to state a claim upon which relief could be granted.[147] Additionally, it invoked foreign sovereign immunity, asserting that the alleged misuse of its software involved foreign governments.[148]

On October 26, 2023, the court granted NSO's motion to dismiss. While it rejected NSO's foreign sovereign immunity defense,[149] it found that the plaintiff had failed to establish personal jurisdiction in Virginia, given insufficient factual evidence that NSO had intentionally targeted her devices in Virginia.[150]

Both parties disputed aspects of the district court's decision, and the case was appealed to the Fourth Circuit. The Khashoggi appeal primarily challenged the jurisdictional ruling, arguing that personal jurisdiction did exist and that NSO

---

[140] Complaint, Khashoggi v. NSO Grp. Techs., No. 1:23-cv-00779 (E.D. Va. Jun. 15, 2023).
[141] *Id.* at 36.
[142] *E.g.*, Oren Liebermann, *How a Hacked Phone May Have Led Killers to Khashoggi*, CNN (Jan. 20, 2019), www.cnn.com/2019/01/12/middleeast/khashoggi-phone-malware-intl/index.html.
[143] Alex Hannaford, *'He Couldn't See Light at the End of the Tunnel': Jamal Khashoggi's Widow on Their Life and His Death*, THE GUARDIAN (Feb. 10, 2024), www.theguardian.com/world/2024/feb/10/he-couldnt-see-light-at-the-end-of-the-tunnel-jamal-khashoggi-widow-on-their-life-and-his-death [https://perma.cc/FAL8-7SLW].
[144] Complaint, Khashoggi v. NSO Grp. Techs., *supra* note 140, at 129.
[145] 18 U.S.C. § 1030.
[146] Va. Code Ann. § 18.2-152 (2026).
[147] Notice of Mot. and Mot. of Defendants to Dismiss Complaint, Khashoggi v. NSO Grp. Techs., No. 1:23-cv-00779 (E.D. Va. Sep. 29, 2023), at 16-26.
[148] *Id.* at 6.
[149] Order re Mot. to Dismiss, *supra* note 139, at 8.
[150] *Id.* at 12.

had purposefully directed its conduct at Virginia.[151] In May 2025, the Fourth Circuit affirmed the district court's decision. The court resolved the case on the issue of personal jurisdiction, as the complaint failed to allege with sufficient specificity where and how long Khashoggi lived in Virginia during the alleged surveillance, and had not adequately alleged that NSO, as opposed to Saudi or UAE government figures, was the entity targeting her. Therefore, the court declined to hold that a Virginia district court should assert specific personal jurisdiction over the case.[152]

American courts have thus largely declined to allow cases filed by individuals against foreign spyware firms to proceed in the United States, with a potential undecided avenue relevant mostly for American citizens or residents who have been targeted outside of the United States. This is primarily due to a lack of personal jurisdiction and the doctrine of *forum non conveniens*. Courts have pointed to Israel as a more appropriate forum for such litigation, calling it the "adequate alternative forum," in the *Corallo* case,[153] the jurisdiction where NSO is amenable to process in the original decision in the *Dada* case,[154] and the place where NSO has witnesses, employees, regulators, and the jurisdiction with a strong national security interest, in the *Khashoggi* case.[155] However, an examination of litigation in Israel suggests that proceedings there have also been largely unsuccessful thus far, perhaps raising questions about the accuracy of courts finding that Israel is an appropriate forum in which to litigate against NSO.

2. In Israel

Examining cases litigated against NSO in Israel can be challenging, as these proceedings are generally conducted behind closed doors and are often subject to gag orders. Several cases filed against NSO in Israel could be identified

---

[151] Brief for Appellant, Khashoggi v. NSO Grp. Techs., No. 23-02234 (4th Cir. Apr. 1, 2024).
[152] Khashoggi v. NSO Grp. Techs., No. 23-02234 (4th Cir. May 21, 2025).
[153] Order Dismissing Action, Corallo v. NSO Grp. Techs., *supra* note 108, at 7.
[154] Order re Mot. to Dismiss, *Dada v.* NSO Grp. Techs., *supra* note 123, at 4-5.
[155] Order re Mot. to Dismiss, *Khashoggi v.* NSO Grp. Techs., *supra* note 139, at 16.

through Nevo,[156] the Israeli court decisions database—equivalent to Westlaw, LexisNexis, or Bloomberg in the United States—and through a review of media reports, but it was usually impossible to view most of the docket. Even for these cases, it was often possible to determine the existence of the case itself, its serial number, the court in which it was filed, the presiding judge, the names of the parties and their attorneys, and, in some instances, some court-issued orders. However, most court records—including protocols, motions, opinions, and judgments—remain subject to gag orders, which are typically issued to protect information deemed of national security significance.[157]

To characterize and analyze litigation against NSO in Israel, I compiled all proceedings I was able to identify through searches of Nevo and Israeli media reports. I identified four such cases, as well as a separate defamation brought by NSO against an Israeli newspaper. I reviewed the publicly available information for each case. Those materials often disclosed the general subject matter and legal claims but did not always reveal the court's disposition or whether a final judgment had been issued.

To supplement this research, I conducted interviews with Eitay Mack and Alaa Mahajna—two private-practice Israeli human rights lawyers who have represented clients against NSO. I also interviewed Yuval Sasson, a partner at the Israeli law firm Meitar LLP.[158] Mr. Sasson asked that no specific case nor client be discussed, and, accordingly, was not asked to comment on any of the particular cases discussed in this Article. However, it has been previously reported in the Israeli press that he represented NSO in Israeli litigation.[159] This section describes litigation against NSO in Israel, synthesizing all publicly

---

[156] NEVO LEGAL DATABASE, www.nevo.co.il (last visited Dec. 15, 2025) (Isr.).

[157] For a comprehensive review of gag orders in Israel, see NOA LANDAU, THE STATE VS. THE PRESS: THE RISE OF GAG ORDERS IN ISRAEL (Reuters Institute at Oxford University, 2016).

[158] משרדי עורכי דין [Law Firms], DUN'S 100 (2024), https://www.duns100.co.il/rating/%D7%93%D7%99%D7%A8%D7%95%D7%92%D7%99%D7%9D/%D7%9E%D7%A9%D7%A8%D7%93%D7%99_%D7%A2%D7%95%D7%A8%D7%9B%D7%99_%D7%93%D7%99%D7%9F [https://perma.cc/83SJ-UD4Y] (last visited Dec. 15, 2025) (Isr.).

[159] Oren Persico, אושרה הגשת תביעה של מתנגד משטר סעודי נגד חברת הריגול הישראלית NSO [A Lawsuit Filed by a Saudi Dissident Against the Israeli Spyware Company NSO Has Been Approved], THE SEVENTH EYE (Dec. 29, 2019), www.the7eye.org.il/355775 [https://perma.cc/GS5D-8UEJ] (Isr.).

available information regarding these cases and drawing on insights from the interviews.

In general, these cases can be classified into two categories. The two cases filed by Mr. Mahajna were brought on behalf of foreign citizens who were allegedly targeted by Pegasus in operations initiated by foreign governments, none of which were Israel. The second category consists of cases filed by Mr. Mack, which were administrative proceedings challenging the Israeli Ministry of Defense's issuance of an export permit to NSO. These cases were not traditional civil actions, but rather administrative proceedings, part of a broader campaign led by Mack to impose stricter regulations on Israeli military exports.

Mr. Mack has litigated numerous cases against the Ministry of Defense over the years, seeking to revoke or restrict export licenses for weaponry and surveillance technology.[160] Among these, two cases appear to have involved NSO. The first dates back to 2017, when Mack petitioned the Israeli Supreme Court, which has original jurisdiction in such matters, seeking to revoke NSO's export permit for Pegasus to Mexico.[161] The petition was based on reports attributing the software's misuse to the Mexican government.[162] The case was litigated behind closed doors, and its details remain subject to a gag order, except for a brief judgment issued in 2018.[163] That judgment reveals that the petitioner was then-Member of Knesset Tamar Zandberg from the left-wing Meretz party.[164] The publicly available portion of the judgment consists of a single sentence:

---

[160] *E.g.*, Judah Ari Gross, עתירה לבג"צ: להשעות ייצוא נשק סייבר ששימש ל"העלמת" סטודנטים [After Court's Gagged Ruling on Arms Sales to Myanmar, Activists Call for Protest], THE TIMES OF ISRAEL (Sep. 28, 2017), www.timesofisrael.com/after-courts-gagged-ruling-on-arms-sales-to-myanmar-activists-call-for-protest [https://perma.cc/U3JE-EB83] (Isr.).

[161] HCJ 5662/17 *Zandberg v. Minister of Defense* (Mar. 20, 2018) (Isr.).

[162] Oded Yaron, *The Secret of NSO's Success in Mexico*, HAARETZ (Nov. 30, 2020), www.haaretz.com/israel-news/tech-news/2020-11-30/ty-article/.highlight/the-secret-of-nsos-success-in-mexico/0000017f-e0f5-d568-ad7f-f3ff5cff0000 [https://perma.cc/TG5K-8GPT].

[163] *Zandberg v. Minister of Defense*, *supra* note 161.

[164] Yaron, *supra* note 162.

"Therefore, the petition is dismissed."[165]

Media reports from 2017 confirm that the petition, filed by Mack on Zandberg's behalf, specifically concerned allegations of Pegasus' abuse in Mexico.[166] According to *Haaretz*, the petition was submitted in response to publications attributing the software's misuse to Mexican authorities, including allegations of infections targeting journalists, members of international investigative committees, and others.[167] In a conversation, Mack confirmed these details and stated that:

"Regarding the [2017] case, I filed a petition to revoke [NSO's] license to [export to] Mexico, due to the revelations about the cases there. There is a gag order on this matter, and it is only permitted to say that the petition was dismissed."[168]

In 2019, Mr. Mack filed another petition in the Tel Aviv District Court on behalf of 30 petitioners, including several members of Amnesty International's Israeli branch at the time.[169] It argued that NSO should not be permitted to sell its Pegasus spyware to foreign governments, citing, among other reasons, a claim that an Amnesty International staff member had been targeted.[170] In July 2020, the court denied the petition, issuing a comprehensive judgment that remains subject to a gag order. However, the court also released a shortened

---

[165] *Zandberg v. Minister of Defense*, *supra* note 161.

[166] John Brown, עתירה לבג"צ: להשעות ייצוא נשק סייבר ששימש ל"העלמת" סטודנטים [A petition to the Israeli Supreme Court: Suspend the export of cyber weapons used to "disappear" students], HAARETZ (Jul. 13, 2017), www.haaretz.co.il/blogs/johnbrown/2017-07-13/ty-article/0000017f-f8bb-d460-afff-fbffb3b90000 [https://perma.cc/GC8D-S3AC] (Isr.).

[167] Id.

[168] Telephone Interview with Eitay Mack, Attorney (Jan. 28, 2025) (on file with author).

[169] AdminA (Tel-Aviv Dist. Ct.) 28312-05-19 Malekar v. DECA, 2 (Jul. 12, 2020) (Isr.).

[170] Omer Kabir, אינטרנשיונל אמנסטי נגד הופעלו NSO של הריגול כלי [NSO's spyware was deployed against Amnesty International], CALCALIST (Aug. 1, 2018), www.calcalist.co.il/internet/articles/0,7340,L-3743502,00.html [https://perma.cc/6QXU-7WEG] (Isr.); Amnesty International, Amnesty International Among Targets of NSO-powered Campaign, AMNESTY.ORG (Aug. 1, 2018), www.amnesty.org/en/latest/research/2018/08/amnesty-international-among-targets-of-nso-powered-campaign [https://perma.cc/JS3U-ZSZZ].

version of the ruling for public access. The publicly available version of the judgment states that:

"The court has been convinced that the regulatory processes . . . are sensitive and stringent, involving a thorough examination of export requests. . . . Licensing is conducted through a rigorous process, and even after a license is issued, the agency maintains close oversight and regulation. If necessary - particularly in cases involving human rights violations - the license may be revoked upon discovering a violation. . . . I find that [the Ministry of Defense] is fulfilling its regulatory duties with diligence . . . in a manner that demonstrates a high level of sensitivity to human rights concerns."[171]

The Pegasus Project was not published until a year later.[172] In retrospect, Mr. Mack contends that the court's decision not only to dismiss the petition but also to commend the Ministry of Defense's regulatory mechanisms now appears "embarrassing":

"In the Amnesty case, in the publicly available judgment, the judge went even further . . .[and] wrote that the Ministry of Defense strictly adheres to human rights considerations in its licensing decisions, that there was no flaw in its conduct, and that it carries out thorough inspections - she was impressed. . . . Shortly afterward, the Pegasus affair exploded. This judge also deviated from the norm, as judges typically do not . . . hand out commendations or praise to public authorities. But she fully backed the Ministry of Defense. . . . In all my other cases related to arms trade, the judgments remained classified. In this instance, the Ministry of Defense actually wanted a public ruling . . . They wanted recognition, and for that reason, they decided there would be one classified judgment and one public judgment - in which the praise appeared. But then the Pegasus affair broke globally, creating an embarrassing situation: what sort of oversight does the court really exercise if the judge declared the system to be so effective, only for the Pegasus scandal to be exposed worldwide?"[173]

---

[171] AdminA (Tel-Aviv Dist. Ct.) 28312-05-19 *Malekar v. DECA*, 2 (Jul. 12, 2020) (Isr.).
[172] The Pegasus Project, *supra* note 51.
[173] Interview with Eitay Mack, *supra* note 168.

In an interview, Mr. Mack added that he had sent letters to the Attorney General and the State Attorney requesting the initiation of a criminal investigation against NSO Group in two other instances: one concerning an alleged deal in Ghana and the other in Hungary. These efforts were also unsuccessful and have not resulted in litigation thus far.[174]

Mr. Mahajna's cases more closely resemble those litigated in the United States, in which foreign individuals brought legal actions. Mr. Mahajna's clients included a Saudi citizen and a group of Mexican journalists, represented in two separate proceedings. According to Mahajna, the lawsuit on behalf of the Mexican journalists was the first to be filed. The case, brought before the Tel Aviv District Court (circuit equivalent), was directed against NSO and an additional spyware company connected to Israel and possibly Cyprus. According to news reports on the matter, the lawsuit was filed on behalf of five Mexican nationals who have been allegedly targeted by Pegasus between 2014 and 2016.[175] An equivalent lawsuit was filed simultaneously in Cyprus and involved a Qatari plaintiff.[176] In an interview, Mahajna stated that the Cyprus case has been dismissed shortly after its filing. The Israeli case, he added, is under a gag order. According to Mahajna, the court has stayed the proceedings, though it has not yet been dismissed. As a result, the case remains largely inactive.[177]

The second case was filed in 2018 in the Tel Aviv Magistrate Court by Omar Abdulaziz Al-Zahrani, a Saudi citizen close to Jamal Khashoggi who currently

---

[174] *Id*.

[175] Lilach Baumer, *Lawsuit Asks to Restrict Sales of Israeli Spyware*, CTECH (Sep. 2, 2018), www.calcalistech.com/ctech/articles/0,7340,L-3745470,00.html [https://perma.cc/HEM2-XYH8]; David D. Kirkpatrick and Azam Ahmed, *Hacking a Prince, an Emir and a Journalist to Impress a Client*, THE NEW YORK TIMES (Aug. 31, 2018), www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html [https://perma.cc/3HMQ-EM38].

[176] Kirkpatrick & Ahmed, *supra* note 175; Amitai Ziv, "עורך הדין": התקשרו עם משטרים אפלים שנלחם בחברת הריגול הישראלית ["They've Engaged with Dark Regimes": The Lawyer Fighting the Israeli Spyware Company], THE MARKER (Sep. 3, 2018), www.themarker.com/technation/2018-09-03/ty-article/0000017f-ed37-ddba-a37f-ef7ff5580000 [https://perma.cc/YFM2-VEPE] (Isr.).

[177] Telephone Interview with Alaa Mahajna, Attorney (Feb. 2, 2025) (on file with author).

resides in Canada.[178] Al-Zahrani alleged that he had been targeted by Pegasus. The plaintiff sought damages of approximately 600,000 New Israeli Shekels (NIS).[179] NSO contested the lawsuit, asserting that it was entirely without merit and lacked any evidentiary foundation. The company moved to dismiss the case, reportedly arguing that "this is a baseless lawsuit in all respects, which on its face does not disclose a cause of action or any legal standing against the defendants and was filed in bad faith."[180]

The court denied the plaintiff's request to issue an injunction preventing NSO from offering its services to foreign governments and ordered him to pay NSO 30,500 NIS in costs.[181] However, the court allowed the remainder of the case to move forward. In December 2019, the magistrate court denied NSO's motion to dismiss the case in its entirety, finding that "It is enough [at this stage] to find that the lawsuit is not baseless on its face."[182] According to a news report, the judge refused to issue a gag order, but the decision no longer seems to be publicly available on legal databases.[183] In an interview, Adv. Mahajna stated that the case remains "stuck" at the early discovery stages. He noted that the Attorney General sought permission to submit a motion that could be described as an equivalent of an amicus brief regarding discovery process, citing the highly sensitive nature of the case, which implicates Israel's security regulations and the extent to which they may have enabled private firms to sell surveillance software to foreign governments.[184]

---

[178] Hagar Shezaf, *Snowden: Israeli Firm's Spyware Was Used to Track Khashoggi*, HAARETZ (Nov. 7, 2018), www.haaretz.com/israel-news/2018-11-07/ty-article/.premium/israeli-spyware-was-used-to-track-saudi-journalist-khashoggi-edward-snowden-says/0000017f-e09f-df7c-a5ff-e2ffc1650000 [https://perma.cc/PU2F-3C26].

[179] Complaint, *Abdulaziz Al-Zahrani* v. *NSO Group*, Civ. Case No. 2401-12-18 (Tel-Aviv Mag. Ct. Feb. 2, 2018) (Isr.) [Hebrew].

[180] Oded Yaron, בית משפט בישראל התיר לחברו של ג'מאל חאשוקג'י לתבוע את NSO Group [An Israeli court allowed Jamal Khashoggi's friend to sue NSO Group], HAARETZ (Dec. 29, 2019), www.haaretz.co.il/captain/software/2019-12-29/ty-article/.premium/00000180-8e03-d6ed-a3e0-fe1747ed0001 [https://perma.cc/MY9Z-4UQH] (Isr.).

[181] *Id*.

[182] Order re Mot. to Dismiss at 3, Abdulaziz Al-Zaharni v. NSO Group, Civ. Case No. 2301-12-18 (Tel-Aviv Mag. Ct. Dec. 22, 2019).

[183] *Id*.

[184] Interview with Alaa Mahajna, *supra* note 177.

In practice, Mahajna contends, private litigants face considerable difficulties in pursuing such proceedings:

"We decided to proceed with the lawsuit in the magistrate's court, and it seemed to be moving forward. But later, during the preliminary proceedings, they kept filing all sorts of . . . appeals on every issue. Then, the Attorney General proposed a framework for disclosing the documents, and we are still stuck there - extensions upon extensions. You could say we are still at the very beginning. . . . *Ordinary people cannot handle lawsuits like this; it is simply impossible. We've seen it in many films, but it happens in reality as well. When you pursue this kind of lawsuit, they can drag you along for years without any substantive progress*."[185]

As mentioned, Yuval Sasson declined to comment on any specific client or case. Instead, he was willing to discuss the broader legal framework governing the commercial spyware industry. According to Mr. Sasson, there are inherent limitations in both the regulation of these companies and the litigation brought against them.

Regarding regulatory oversight, Sasson emphasized that an exclusive focus on privacy rights risks creating a regulatory failure, as regulators must also account for competing considerations, including national security and foreign affairs. However, the fact that regulatory mechanisms incorporate these broader considerations creates a paradox, in his opinion: firms such as NSO operate under the oversight of state regulators, yet they receive no protection when those regulators fail. "The regulation is often irrelevant," Sasson argues, noting that spyware firms face liability for the misuse of their products in ways that manufacturers of conventional weaponry do not.

According to Mr. Sasson, the intense public scrutiny surrounding the spyware industry places significant pressure on governments—such as the Israeli government in the Pegasus case—but these governments often fail to respond effectively:

---

[185] *Id*.

"Then [the public pressure] reaches governments, and they don't know what to do with it. And that puts pressure on [the government], and they don't know how to handle it. So, they place the responsibility on the [spyware] companies. And this responsibility is, first of all, in retrospective. And second, [the spyware firms] have no way to control it. The only way is to give authority to certain regulatory bodies to oversee what states are doing. But it's clear that this is an undesirable outcome. . . So, essentially, [the spyware companies] fall into a situation where there is an unclear regulatory vacuum, and the regulation is shaped solely by the test of consequences. And the test of consequences is: who gets caught. . . . No one is asking whether Italy wiretapped politicians and journalists or not. The only question is whether it's Cellebrite or Paragon [who provided a program that could have allowed governmental surveillance]. The only issue is that WhatsApp sends a letter to Paragon. WhatsApp didn't write to the Italian government; no one will sue the Italian government."[186]

In other words, Sasson contends that holding spyware firms liable for abuses committed by governments—abuses that these firms allegedly could neither have predicted nor prevented—constitutes a fundamental legal failure:

"The regulatory failure begins with the question of who is being supervised in the first place. And when the supervision is placed on an entity that doesn't have the tools for [enforcement] - it's not even [given the authority to serve as] a gatekeeper. It's not like what was done with banks, where privatization [of certain aspects of law enforcement, for instance around money laundering] was done. It's without authority. We told the banks, for instance: 'You will be the gatekeepers for money laundering issues, we transferred the responsibility, and turned every bank clerk into a tax collector. They have responsibility, but they also have authority. They can refuse to open a bank account. Here, [with the spyware companies] you're telling these [spyware] companies not to sell."[187]

The complex relationship between spyware firms and the Israeli government, along with its regulatory agencies, also limits these firms' ability to adequately defend themselves in legal proceedings outside of Israel,

---

[186] Online Interview with Yuval Sasson, Partner, Meitar (Mar. 4, 2025).
[187] *Id*.

according to Mr. Sasson. The central issue, he argues, is that Israeli agencies impose strict confidentiality requirements that prevent spyware firms from disclosing information that may be critical to their legal defense in foreign jurisdictions. This creates a situation in which these companies are unable to effectively litigate abroad. In other words, if a U.S. court asserts personal jurisdiction over a firm like NSO, the company would—according to Adv. Sasson—face an "impossible dilemma": either comply with Israeli legal and regulatory mandates prohibiting the disclosure of classified information, including proprietary code deemed essential to national security and lose the case; or disclose such information in an effort to prevail in litigation, risking relationships with the Israeli government, and potentially the state's national security interests.[188]

To clarify, the argument presented here, based on this body of litigation, does not claim that Israel is categorically incapable of providing any remedy. Although Israel has evidently proven to be an unfavorable forum for plaintiffs in this space at the time, the existing record does not (yet) establish that Israeli courts are unable to provide any remedy at all. Accordingly, while this analysis may give rise to certain counterarguments against the forum non conveniens determinations, especially in light of changes NSO has undergone, including the appointment of a new chairman, [189] it does not suggest that those counterarguments would prevail. It does show, however, that individual plaintiffs have faced serious obstacles when attempting to litigate in Israel, and that this potential avenue of litigation is not currently likely to provide an effective means of practically regulating or mitigating the commercial spyware industry.

B. U.S. Litigation by Tech Giants

In the United States, another category of litigation against NSO Group has emerged: cases initiated by major technology companies. The two principal

---

[188] Telephone Interview with Yuval Sasson, Partner, Meitar (Mar. 10, 2025).
[189] Wrobel, *supra* note 76.

cases in this category are *Apple v. NSO*[190] and *WhatsApp v. NSO.*[191] In addition, as previously noted, certain tech giants have also filed amicus briefs in *Dada v. NSO*.[192] Unlike lawsuits brought by individuals, litigation initiated by technology companies is structured around a distinct set of legal claims, follows a difference procedural path, and, in at least one instance, has achieved some measure of success.[193] To provide a clear analytical framework, this section will begin by examining the *Apple* case before turning to the *WhatsApp* litigation.

One of the methods by which Pegasus operated at a certain stage was through a vulnerability in Apple's iPhones, known as FORCEDENTRY.[194] On November 23, 2021, Apple filed a complaint against NSO Group in the U.S. District Court for the Northern District of California, alleging that NSO "abused Apple services and servers to perpetrate attacks on Apple's users and data stored on users' devices."[195] According to the complaint, NSO "misused Apple ID accounts to send abusive commands to Apple servers [and] misused Apple servers to deploy malware and attack Apple users."[196]

The complaint tried to navigate an evidently challenging balance, asserting that NSO's actions caused significant harm by exploiting vulnerabilities in Apple's products, all the while simultaneously highlighting the purported security of Apple devices compared to competitors.[197] The lawsuit also offered insight into Apple's understanding of how Pegasus was used to target its users. Apple's claims relied on technical findings published by the Citizen Lab in its assessment of the spyware and the FORCEDENTRY exploit.[198] As Apple stated in

---

[190] Order re Voluntary Dismissal and Sealing, Apple Inc. v. NSO Grp. Techs., No. 3:21-cv-09078 (N.D. Cal. Nov. 12, 2024).
[191] Order re Mot. for Summ. J., Motion for Sanctions, and Discovery Letter Briefs, WhatsApp Inc. v. NSO Grp. Techs., *supra* note 7.
[192] Brief for Microsoft Corporation, Google LLC et al. as Amici Curiae Supporting Plaintiffs-Appellants, WhatsApp LLC v. NSO Grp. Techs., No. 20-16408 (9th Cir. Dec. 21, 2020).
[193] Order re Mot. for Summ. J., Motion for Sanctions, and Discovery Letter Briefs, WhatsApp v. NSO Grp. Techs., *supra* note 7.
[194] Marczak et al., *supra* note 111.
[195] Complaint at 2-3, Apple Inc. v. NSO Grp. Techs., No. 3:21-cv-09078 (N.D. Cal. Nov. 23, 2021).
[196] *Id.* at 7.
[197] *E.g.*, *id.* at 3, discussing Android's vulnerabilities.
[198] Marczak et al., *supra* note 111.

its complaint, NSO would contact Apple servers in the United States and abroad to identify other Apple devices and would then send "abusive data" through Apple servers to initiate the attack.[199]

Apple alleged violations of the CFAA,[200] the California Business and Professions Code,[201] breach of contract, and unjust enrichment. For several months, however, the case remained largely stagnant, as both parties requested that the court hold proceedings in abeyance pending a ruling on the jurisdictional issues in *WhatsApp v. NSO*, which had been filed earlier. It was not until January 23, 2024 that the district court ruled on NSO's jurisdictional argument, rejecting it and finding, unlike in cases brought by individual plaintiffs, that the burdens imposed on NSO in litigating the case in California were comparable to those Apple would face if required to litigate in Israel. The court held that "NSO has not met its heavy burden of demonstrating that the circumstances of this litigation warrant dismissal on forum non conveniens grounds."[202]

This ruling led to the denial of NSO's motion to dismiss. More than two years after the lawsuit was filed, NSO was required to respond to the complaint. Its answer, filed on February 14, 2024, broadly denied most of Apple's key allegations.[203] The case then proceeded to the discovery phase.

On November 12, 2024, however, Apple filed a motion for voluntary dismissal, claiming NSO had become significantly weakened since the lawsuit was initiated and no longer posed a substantial threat to Apple's software.[204] Apple also expressed concerns that the discovery process could compromise its broader security efforts. Apple's lawsuit's ultimate dismissal brings us to the

---

[199] Complaint, *Apple v. NSO, supra* note 195, at 14.
[200] 18 U.S.C. § 1030.
[201] Cal. Bus. & Prof. Code § 17200.
[202] Order re Mot. to Dismiss and Further Proceedings, Apple Inc. v. NSO Grp. Techs., No. 3:21-cv-09078 (N.D. Cal. Jan. 23, 2024).
[203] Answer of Defendants NSO Group Technologies Limited and Q Cyber Technologies Limited, Apple Inc. v. NSO Grp. Techs., No. 3:21-cv-09078 (N.D. Cal. Feb. 14, 2024).
[204] Apple's Mot. to Voluntary Dismiss, Apple Inc. v. NSO Grp. Techs., No. 3:21-cv-09078 (N.D. Cal. Nov. 12, 2024).

only case I have identified that has, thus far, resulted in a substantive legal outcome against NSO Group in the United States: *WhatsApp v. NSO*.[205]

WhatsApp, a messaging application owned by Meta, originally filed suit against NSO Group on October 29, 2019. The complaint set forth four causes of action: violation of the CFAA; violation of the California equivalent, the California Comprehensive Computer Data Access and Fraud Act (CDAFA); breach of contract; and trespass to chattels.[206] In the beginning, certain experts criticized the lawsuit, deeming it mostly an exercise in public relations that relied too heavily on terms of service and offered a problematic interpretation of the CFAA.[207] Others, prominently Penney and Schneier, found greater merit in it, emphasizing that "on the facts of the case, a fairly straightforward application of the CFAA would find that [NSO] were liable,"[208] an idea they supported as an opportunity to improve corporate accountability.[209] In hindsight, as of today, it seems that their argument has generally proven itself in court.

On July 16, 2020, the district court found that it had jurisdiction over the case, concluding that NSO had deliberately sought out and accessed WhatsApp's servers.[210] The court further determined that NSO had "*reverse-engineered the WhatsApp app and developed a program that emulated legitimate WhatsApp network traffic in order to transmit malicious code over WhatsApp servers*." In its ruling, the court rejected NSO's claim of foreign official or derivative sovereign immunity. However, it also dismissed WhatsApp's trespass to chattels claim.[211] In dismissing the trespass claim, the court relied on *Intel v. Hamidi*, a 2003 decision by the Supreme Court of California, which

---

[205] Order re Mot. for Summ. J., Motion for Sanctions, and Discovery Letter Briefs, WhatsApp Inc. v. NSO Grp. Techs., *supra* note 7.
[206] Complaint at 10-13, WhatsApp Inc. v. NSO Grp. Techs., No. 4:19-cv-07123 (N.D. Cal. Oct. 29, 2019).
[207] Jonathon W. Penney & Bruce Schneier, *Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group*, 36 BERKELEY TECH. L.J., 469, 477 (2021).
[208] *Id.* at 478.
[209] *Id.* at 510.
[210] Order Granting in Part and Denying in Part Mot. to Dismiss and Denying Mot. to Stay Recovery, WhatsApp Inc. v. NSO Grp. Techs., No. 4:19-cv-07123 (N.D. Cal. Jul. 16, 2020).
[211] *Id.* at 44.

held that emails sent by a former Intel employee to current employees of the company did not constitute trespass.[212]

NSO appealed the jurisdictional ruling to the Ninth Circuit, once again asserting that the case should be dismissed.[213] A number of technology companies and other organizations submitted amicus briefs in support of the district court's jurisdictional ruling.[214] The Ninth Circuit ultimately rejected NSO's arguments and affirmed the lower court's decision.[215] NSO then petitioned the Supreme Court for a writ of certiorari.[216] On January 9, 2023, the Supreme Court declined to grant certiorari, thereby leaving the Ninth Circuit's ruling intact.[217]

Following the Supreme Court's denial of review, the case returned to the district court for further litigation. Eventually, on December 20, 2024, the district court granted summary judgment in favor of WhatsApp, marking the first time NSO had been found liable in a U.S. court.[218] In its decision, the court held NSO liable on the three remaining causes of action. The court conducted a detailed analysis of the evidence regarding Pegasus's functionality and determined that its use violated WhatsApp's terms of service and constituted a violation of the CFAA and the CDAFA.[219] With respect to the breach of contract claim, the district court held that NSO had violated WhatsApp's terms of service.[220] With liability established, a jury then awarded WhatsApp

---

[212] *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003).

[213] WhatsApp LLC v. NSO Grp. Techs., No. 20-16408 (9th Cir. July 22, 2020).

[214] Brief of Microsoft Corporation, Google LLC et al. as Amici Curiae Supporting Plaintiffs-Appellants, WhatsApp LLC v. NSO Grp. Techs., No. 20-16408 (9th Cir. Dec. 21, 2020); Brief of Access Now, Amnesty International et al. as Amici Curiae Supporting Appellee's Request for Affirmance, WhatsApp LLC v. NSO Grp. Techs., No. 20-16408 (9th Cir. Jan. 7, 2021).

[215] WhatsApp LLC v. NSO Grp. Techs., No. 20-16408 (9th Cir. Nov. 8, 2021).

[216] Pet. for Writ of Cert., NSO Grp. Techs., Ltd. v. WhatsApp Inc., No. 21-1338 (U.S. Apr. 6, 2022).

[217] NSO Grp. Techs., Ltd. v. WhatsApp Inc., No. 21-1338 U.S. (2023) (cert. denied).

[218] Order re Mot. for Summ. J., WhatsApp Inc. v. NSO Grp. Techs., Ltd., No. 4:19-cv-07123 (N.D. Cal. Dec. 20, 2024).

[219] *Id.* at 2, 13. As briefly mentioned, the CFAA analysis was subject to debate among scholars after the lawsuit had been filed. For in-depth analysis in this regard, see Penney & Schneier, *supra* note 207; see also Lubin, *supra* note 4.

[220] *Id.* at 13-14.

$167,245,000 in punitive damages, and an additional $444,719 in compensatory damages.[221]

Following the jury verdict, NSO submitted a motion for remittitur, while WhatsApp moved for a permanent injunction against NSO's operations targeting WhatsApp's platforms. The court has granted both motions at least partially.[222]

As to the injunctive relief, the order was meant to protect WhatsApp from future attacks, but also found that it must "narrow the scope of injunction to apply only to the WhatsApp Platform" itself, and not to other Meta products.[223] Further, it found that the order must "exclude defendants' sovereign government customers from the scope of the injunction."[224]

As to the motion for remittitur, the court granted the motion, and reduced the punitive damages award substantially, from $167 million to merely $4 million.[225] Plaintiffs accepted the remittitur on October 31, 2025, and the court signed its final judgment on November 12, 2025.[226] NSO has nonetheless filed a notice of appeal. According to the reply in support of motion to stay the permanent injunction, NSO argued against both liability and the injunction.[227]

This sequence of events illustrates the nuanced significance of the litigation against NSO. On the one hand, *WhatsApp v. NSO* was the first major case in which, at least at the district court level, a Big Tech company prevailed against a commercial spyware firm. In that respect, the case may be understood as a major moment of standard setting or enforcement in this domain.[228] At the

---

[221] Jury Verdict, WhatsApp Inc. v. NSO Grp. Techs., Ltd., No. 4:19-cv-07123 (N.D. Cal. May 6, 2025).
[222] Order re Mot. for Perm. Inj. & Mot. for Remittitur, WhatsApp Inc. v. NSO Grp. Techs., Ltd., No. 4:19-cv-07123 (N.D. Cal. Oct. 17, 2025).
[223] *Id.* at 18.
[224] *Id.*
[225] *Id.* at 25.
[226] Final Judgment, WhatsApp Inc. v. NSO Grp. Techs., Ltd., No. 4:19-cv-07123 (N.D. Cal. Nov. 12, 2025).
[227] Reply in Support of Mot. to Stay Perm. Inj., WhatsApp Inc. v. NSO Grp. Techs., Ltd., No. 4:19-cv-07123 (N.D. Cal. Dec. 3, 2025).
[228] Davidson, *supra* note 5, at 521.

same time, the court's remittitur decision substantially limited the financial consequences for NSO, making the judgment far less severe, and therefore not necessarily as deterrent, at least from a purely financial perspective.

In this regard, the litigation reveals both the promise of this enforcement mechanism and its limits. That dual insight supports viewing the outcome of *WhatsApp v. NSO*, at least at this stage and following the conclusion of the district court proceedings, as grounds for cautious optimism about the potential of litigation initiated by technology companies against spyware firms. WhatsApp succeeded in overcoming the jurisdictional barriers that had constrained prior litigation brought by individual plaintiffs. It also overcame the practical and procedural burdens of litigating the case itself, including discovery-related obstacles, and, unlike Apple, pursued the litigation through judgment at the district court level and obtained actual compensation.

The difference between WhatsApp and Apple, in this respect, was first and foremost WhatsApp's willingness to litigate the case to completion despite the obvious obstacles. When Apple sought dismissal of its lawsuit, it argued that NSO had become substantially weakened.[229] WhatsApp, apparently, was not persuaded by any similar line of reasoning. The difference between these two strategies may stem from technical considerations or case-specific strategy, but it may also reflect a difference in litigation culture. Any effort to evaluate the future potential of litigation by technology companies against spyware firms must therefore also evaluate the litigation culture and strategic commitments of future plaintiffs, especially the extent to which Big Tech companies will be willing to pursue such litigation to its fullest extent. In other words, the capacity of technology companies to serve as de facto regulators depends not only on their legal ability to bring these suits, but also on their willingness to assume that role despite the burdens and risks litigation entails.

The damages trajectory in WhatsApp further underscores this ambivalence. The jury initially awarded damages at a level that could have carried serious deterrent implications. The court, however, granted NSO's motion for remittitur and reduced the award to an amount with far more limited deterrent force. That

---

[229] Apple's Mot. to Voluntary Dismiss, *supra* note 206.

result suggests that litigation can succeed, but also that its regulatory capacity may be meaningfully constrained by ordinary remedial doctrines. Courts, too, should be attentive to the broader implications of remittitur in this setting if they wish to preserve litigation as a viable complementary regulatory mechanism in the commercial spyware space. This point also responds to the concern that *WhatsApp v. NSO* should be treated not simply as a victory, but as a mixed precedent whose broader significance depends on how one evaluates both its doctrinal success and its practical limits.

III. REGULATION THROUGH LITIGATION

NSO Group offers an illustration of how commercial spyware firms have largely evaded effective traditional regulation.[230] This Section advances two central arguments. First, it agrees with prior scholarship that traditional regulatory frameworks have proven inadequate to prevent the misuse of commercial spyware, particularly from a human rights perspective.[231] It offers several observations as to why these limits are built into the structure of a state-sponsored, national-security-oriented regulatory apparatus, and supports the claim that complementary regulatory mechanisms may be especially useful in this domain.

Second, this Section argues that litigation can function as one such complementary regulatory tool in contexts where state oversight has fallen short. It further examines how future litigation strategies might be structured to make that tool more effective. Based on an analysis of court dockets, this Section supports the argument that Big Tech can beneficially serve as a complementary regulator in this domain.[232] It then evaluates how both technology-company litigation and, potentially, litigation brought by individual

---

[230] *Id.* at 14-22 (discussing various sources of international legal norms and their shortcomings in the context of regulating commercial spyware).
[231] *E.g.*, *id.*; Goldschmidt, *supra* note 95. *See also* Elaine Korzak, *The Key Challenges of Governing Commercial Spyware*, LAWFARE (Jan. 5, 2026), https://perma.cc/8CUU-WB95.
[232] Davidson, *supra* note 5, at 517-26.

plaintiffs may contribute to broader efforts to improve the regulation of commercial spyware.

A. The Limits of Traditional Regulatory Frameworks

Commercial spyware has been widely abused, despite—in the Israeli context—not having been sold in violation of local regulatory requirements. Pegasus is a paradigmatic example. While extensive investigative reporting has documented the misuse of Pegasus by governments across the globe, NSO Group's sales were conducted in compliance with Israeli export regulations.[233] Courts that have reviewed these regulations have even commended their rigor.[234] Institutionally, these regulatory mechanisms are not structured to effectively prevent the abuse of commercial spyware on a global scale with regard to human rights abuse. Three structural limitations make this outcome nearly inevitable.

1. Tension Between National Security and Human Rights

Pegasus was sold internationally in full compliance with Israeli law; there is no credible claim that its export violated Israel's Defense Export Control Act, for instance.[235] This means that DECA approved NSO's sales to foreign governments and vetted their clients in accordance with the dual-stage licensing structure established under Israeli law.[236] Given the extensive reports of Pegasus's misuse, two primary explanations emerge for why these exports were permitted: either DECA failed to accurately assess the potential for misuse, suggesting a lack of resources or expertise—a point I will address later in this section—or it simply did not prioritize human rights considerations when granting export approvals.

---

[233] Bergman & Mazzetti, *supra* note 50; Chin-Rothmann, *supra* note 9.
[234] *Malekar v. DECA*, *supra* note 169.
[235] *E.g.*, Chin-Rothman, *supra* note 9; interviews with Adv. Sasson, *supra* notes 186, 188.
[236] Israel's Defense Export Control Law, *supra* note 48; Goldschmidt, *supra* note 95.

Examination of Israel's Defense Export Control Act could support this explanation. Article 8 of the Act authorizes DECA to deny an export license based on several factors, including an applicant's criminal record, prior violations of the Export Control Act, non-compliance with regulatory requirements, the nature of the exported equipment, knowledge, or service, and considerations related to the end-user.[237] Any evaluation of potential human rights abuses would therefore have to mostly be conducted through DECA's assessment of the end-user.

The legislative history of the Act further illustrates that DECA was designed primarily to serve, first and foremost, Israel's national security and diplomatic interests, rather than to function as a safeguard against human rights abuses. The explanatory notes accompanying the original bill emphasized that export restrictions should be guided by considerations of national security.[238] DECA's official Hebrew-language webpage does reference human rights as a third factor in export decisions after national security and foreign policy considerations.[239]

In other words, the legislature and the executive in Israel deliberately positioned DECA within the Ministry of Defense and granted it regulatory authority to safeguard Israel's national security and foreign relations interests. It may serve also as a human rights watchdog, but it is not designed to prioritize human rights over national security.

This does not mean that the Israeli government is necessarily indifferent to human rights concerns or that DECA entirely lacked the authority to restrict exports based on human rights considerations. In fact, one could argue that human rights abuses sometimes contradict Israel's national security interests, particularly given the diplomatic fallout that follows publications such as the Pegasus Project. However, the structural reality is that DECA was not designed

---

[237] Israel's Defense Export Control Act, *supra* note 48, at art. 8.

[238] Explanatory Notes, Israel's Defense Export Control Bill, Governmental Legislative Proposals 274, 186, 196 (Dec. 19, 2006), www.fs.knesset.gov.il//17/law/17_ls1_566555.pdf [Hebrew] (Isr.).

[239] *Goals*, DECA, www.exportctrl.mod.gov.il/About/Pages/Goals.aspx (last accessed Dec. 15, 2025) [Hebrew].

to prioritize human rights over national security and diplomatic objectives when these considerations are in conflict.[240]

2. The Jurisdictional Challenge

An entirely different set of constraints limiting the ability of regulatory agencies to oversee the export of commercial spyware arises from jurisdictional challenges. Existing regulatory frameworks were originally designed to control the sale and transfer of physical systems. As the explanatory notes to the bill that later became Israel's Export Control Act indicate, prior to the Act's enactment, export controls primarily governed tangible defense equipment such as military hardware, rockets, and related services.[241] These types of exports require extensive physical infrastructure. Strict regulations can deter companies without a serious threat of them relocating to another jurisdiction, because moving production facilities abroad is costly and diplomatically challenging.

This, however, is not the case when the regulated product is software. Firms developing commercial spyware can relocate relatively easily if domestic regulations become too strict. The Export Control Act does mention that Israeli citizens are subject to its regulation,[242] but this relocation opportunity has already been reportedly seized in the Israeli context before. As Lubin observes, commercial spyware companies "are routinely bought and sold, they move, rebrand, and restructure."[243] As a result, they are even more prone to use any gaps and differences between domestic regulatory laws and rules across jurisdictions.[244]

For example, according to media reports, the spyware firm Intellexa developed and sold spyware named Predator, which was allegedly misused for

---

[240] Goldschmidt, *supra* note 95; Tehila Schwartz Altshuler et al., Position Paper for Discussion in the Foreign Affairs and Defense Committee Following the "Pegasus" Affair 16 (2021), www.idi.org.il/media/16676/pegasus.pdf [Hebrew].
[241] Explanatory Notes, *supra* note 238, at 186.
[242] Israel's Defense Export Control Act, *supra* note 48, art. 14.
[243] Lubin, *supra* note 4, at 825.
[244] *Id.* at 825-26.

surveillance operations.[245] Intellexa was founded by two senior veterans of Israel's intelligence services and even reportedly maintained ties to former Prime Minister Ehud Olmert at a certain point.[246] Although Israel's Defense Export Control Act states that an Israeli citizen, resident, or corporation cannot export defense-related knowledge or services without a license,[247] press reports indicate that Intellexa conducted its operations from abroad and, accordingly, did not seek the required export licenses from Israeli authorities.[248] Moreover, a report by the European Parliament found that after Cypriot authorities launched an investigation into Intellexa's activities, the company relocated to Greece.[249] This is just an example, and according to Lubin, over two dozen Israeli spyware companies are registered in Cyprus, where "export control are relaxed."[250]

The non-physical nature of spyware, combined with its mobility, may place regulators in a difficult position. Even if a regulatory agency is committed to addressing human rights concerns, it faces a structural limitation: if the regulatory framework is too strict, spyware companies can relatively easily move their operations elsewhere. This creates an incentive for regulators to adopt a more lenient approach.

A related limitation of existing regulatory frameworks is their exclusive focus on the exportation of surveillance tools, rather than on their domestic use. The case of Pegasus exemplifies this regulatory blind spot. While Pegasus was subject to Israeli export controls, the Israeli police used the spyware domestically, and according to certain reports, engaged in abusive practices

---

[245] Press Release, supra note 33.
[246] Daniel Dolev, *Ehud Olmert Collaborated with Israeli Commercial Spyware Firm Intellexa*, HAARETZ (Oct. 5, 2023), https://perma.cc/8E3X-AJJT [Hebrew].
[247] Israel's Defense Export Control Act, *supra* note 48, art. 14.
[248] Dolev, *supra* note 246.
[249] Ottavio Marzocchi & Emily Ai Hua Gober, *Briefing for the Pega Mission to Cyprus and Greece*, POLICY DEPARTMENT FOR CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS, EUROPEAN PARLIAMENT, at 45 (Nov. 2022), www.europarl.europa.eu/RegData/etudes/STUD/2022/738330/IPOL_STU(2022)738330_EN.pdf.
[250] Lubin, *supra* note 4, at 826.

within Israel, too.[251] A subsequent inquiry by the Israeli Ministry of Justice concluded that the Israeli police deployed Pegasus without proper legal authorization in certain cases.[252] The potential for a government to misuse a domestically developed spyware tool is, by definition, not addressed by agencies responsible for export controls. As a result, such practices remain largely unregulated.

3. Limited Institutional Expertise and Resources

DECA operates as an integral part of the Israeli Ministry of Defense and is staffed primarily by individuals with backgrounds in national security. For example, the head of the agency as of early 2026, Racheli Chen, has spent her career in various positions within the Ministry of Defense, including roles in the Administration for Weapon Development and Technological Infrastructures, the Budget and Transactions Unit, and the Unmanned Aerial Vehicles Directorate.[253]

However, DECA's primary mission does not center exclusively on cybersecurity. According to data from the Ministry of Defense, cyber and information intelligence tools accounted for 4% of Israel's defense exports in 2023.[254] The vast majority of DECA's work focuses on more traditional defense technologies rather than cyber-surveillance tools. Furthermore, DECA is responsible for overseeing an immense volume of transactions. In 2023 alone, it oversaw defense deals worth over $13 billion.[255]

This challenge is further compounded by a potential lack of sufficient technical expertise. Commercial spyware is an exceptionally sophisticated and highly secretive industry. These tools are designed to be constantly evolving,

---

[251] Merari et al., *supra* note 30.
[252] Tomer Ganon, *NSO Group at the Service of the Israeli Police: Hacking Citizens' Phones Without Oversight or Control*, CALCALIST (Jan. 18, 2022), https://perma.cc/2Z9N-ZQH7 [Hebrew]; Merari et al., *supra* note 30.
[253] Yuval Azulai, *Racheli Chen appointed Export Controls Agency head*, GLOBES (Sep. 6, 2016), https://perma.cc/7ZZG-X8S7.
[254] Press Release, For the third consecutive year: A new all-time record in Israel's defense exports—over $13 billion in 2023 (approximately 49 billion ILS), ISRAEL'S MINISTRY OF DEFENSE (Jun. 16, 2024), www.perma.cc/HN49-GRV3.
[255] Id.

adapting to new vulnerabilities, and circumventing security measures.[256] In theory, effective oversight would require not only access to the source code of these products but also personnel with advanced cybersecurity expertise capable of independently evaluating the spyware's capabilities. Skilled vulnerability assessors are in high demand and command competitive salaries, even within Israel's thriving high-tech sector.[257]

A similar limitation stems from the fact that, by design, these products are regulated only after they have already been developed. Accordingly, by the time oversight mechanisms even consider whether to license a particular spyware product, the intrusive technology already exists and is likely operational.[258] This structure makes meaningful regulation more difficult. Once the product has been built, deployed, or made available for deployment, regulators are no longer deciding whether such a capability should come into existence in the first place. Instead, they are attempting to regulate, mitigate, or limit the use of an already-existing surveillance tool retrospectively, after the relevant technological capacity has already been created.

It is far from clear, then, that a public-sector agency, operating within Israel's bureaucratic constraints, has the technical capacity to properly assess the spyware it reviews, let alone to predict how offensive its capabilities may become as new vulnerabilities are discovered and exploited. The structural disparity between the well-resourced spyware firms and the regulatory agency tasked with overseeing them creates an inherent imbalance of power, which may lead to a more permissive regulatory approach. Indeed, DECA was forced to modify its cyber export policies only after the revelations of the Pegasus Project—suggesting that it may not have been fully aware of how the products it authorized for export were being used in practice.[259] Given these realities,

---

[256] E.g., Bill Marczak, John Scott-Railton, Bahr Abdul Razzak, & Ron Deibert, Triple Threat: NSO Group's Pegasus Spyware Returns in 2022 with a Trio of iOS 15 and iOS 16 Zero-Click Exploit Chains, THE CITIZEN LAB (Apr. 18, 2023), www.citizenlab.ca/2023/04/nso-groups-pegasus-spyware-returns-in-2022.

[257] E.g., Yoav Cohen, "Always Stay One Step Ahead of the Hacker": What Does a Vulnerability Researcher Do?, HAARETZ (Jun. 13, 2023), https://perma.cc/8UD9-DPW4.

[258] Lubin, supra note **Error! Bookmark not defined.**, at 825.

[259] E.g., Assaf Gilad, The changes in defense export regulations are creating challenges for Israeli cyber companies, GLOBES (Apr. 25, 2022), https://perma.cc/FH5V-SP5S.

DECA's capacity to regulate commercial spyware in a manner that effectively prevents human rights abuses is somewhat questionable, both in terms of expertise and available resources.

The ideas and arguments presented here apply most directly to the Israeli regulatory context because that framework was the primary avenue through which the export of Pegasus around the world could have been regulated. The failure of traditional regulatory mechanisms to oversee this domain, however, and the limitations identified here, are not necessarily limited to Israel. As noted above, companies based in other jurisdictions also develop and sell spyware tools.[260] Israel is certainly not the only government that may have incentives to prioritize national security interests and diplomatic advantages when making export-control licensing decisions over due process, privacy, or human rights concerns in other countries.

The knowledge and expertise gap may likewise characterize the relationship between sophisticated technology companies and governmental agencies in this field. And, of course, the nature of the industry itself, including its geographic flexibility and its capacity to relocate to more favorable jurisdictions when regulation becomes too burdensome, is a feature of commercial spyware and its products rather than of any particular company discussed here. As a result, the argument presented here is not that any specific Israeli regulatory agency is necessarily an extreme or uniquely deficient example. Rather, the argument is that broader, built-in flaws may arise by design whenever a state entrusts an agency that is functionally part of the national security apparatus with the task of effectively regulating the export or use of commercial spyware.

B. Regulation Through Litigation and Big Tech's Role

A complementary regulatory mechanism for mitigating the human rights abuses associated with commercial spyware may be found in litigation. As this Article surveys, litigation appears to offer a potentially viable avenue in at least some cases. These suits, however, seem most likely to move forward when they

---

[260] E.g., Roberts et al., supra note 16, at 10-11.

are brought by, or at least supported by, major technology companies in the United States. This Section therefore examines the potential role of technology companies as de facto regulators in this space. It first explores why technology companies are relatively well-positioned to engage in such litigation. It then turns to the question whether these companies have sufficient incentives to actively pursue litigation as a complementary regulatory strategy.

1. Tech Giants' Unique Regulatory Position

Unlike state-sponsored regulators, whose capacity to oversee and constrain the industry is limited by structural, jurisdictional, and national security considerations, tech giants operate largely independently of these constraints. At the same time, they often do not face the limitations and structural disadvantages encountered by individuals targeted by spyware. This unique positioning allows tech giants to leverage legal action as a means of imposing meaningful constraints on commercial spyware firms, filling a critical regulatory gap.

a) In Comparison with Traditional, State-Operated Regulation

The Pegasus case study highlights at least three structural limitations that state-sponsored regulatory agencies face in overseeing commercial spyware. First, there is an inherent tension between national security and foreign affairs interests, on the one hand—which agencies such as DECA are designed to protect—and the imperative to prevent human rights abuses on the other hand. Second, there is a dual jurisdictional challenge: spyware firms can relocate relatively easily, compared to other defense-oriented industries, to avoid strict regulations. In addition, agencies such as DECA typically have oversight authority only over the export of such tools, leaving them unable to prevent their abuse within the jurisdiction in which they were developed. Third, these agencies may lack the necessary expertise—both technical and in human rights as a discipline—as well as the resources needed to effectively regulate these programs.

Technology companies, by contrast, do not face these same limitations, at least not to the same extent as state-sponsored regulators. Unlike government agencies, their primary concern is neither national security nor diplomacy but rather their business interests, which require the integrity of their platforms, the trust of their users, and the long-term sustainability of their business models. While they may collaborate with national security agencies, they are not structurally bound by the same incentives that constrain state regulators. As a result, tech giants may be better positioned to mitigate human rights abuses associated with commercial spyware firms, serving as a crucial counterweight to the limitations of traditional regulatory frameworks.

Tech giants may be better positioned than state-centered regulators to balance the competing interests of national security, foreign relations, and human rights, at least in the sense that they are not institutionally designed to prioritize national security over all other considerations. To be sure, these firms are far from indifferent to national security concerns. Many collaborate with national security agencies, and their leadership may have ideological, institutional, or business incentives to align with U.S. national security priorities,[261] as well as with the interests of other governments. This concern may be especially salient in the present moment, given shifting political conditions that some commentators argue may produce closer alignment between Big Tech and governmental interests.[262] In a sense, under any democratic government, private actors such as Big Tech must navigate competing incentives. On the one hand, they may seek to maintain close relationships with the government, and in particular with the national security apparatus. On the other hand, they also have incentives to present themselves as protective of their users, resistant to abusive surveillance, and committed to privacy, particularly when they are portrayed as surveillance intermediaries, privacy champions, or defenders of civil liberties.[263] As noted above, Big Tech's

---

[261] *E.g.*, Alex C. Karp & Nicholas W. Zamiska, The Technological Republic 51-53 (2025).

[262] *E.g.*, Blake Montgomery, *Big tech continues to bend the knee to Trump a year after his inauguration*, The Guardian (Jan. 20, 2026), https://perma.cc/U85P-HH77; Paul M. Barrett, *Tech's Love Affair with Trump Grows Stronger By the Day*, Tech Pol'y Press (Oct. 23, 2025), https://perma.cc/5X4M-PE6S.

[263] Rozenshtein, *supra* note 6.

potential advantage over state-sponsored regulators in the commercial spyware context exists only so long as these companies retain incentives not to become fully embedded within the state's national security communities and mechanisms. It is often public opinion, investigative journalism, civil society pressure, and the expectations of Big Tech's users that could help create and sustain those incentives.

However, these firms are not embedded within the national security establishment, conceptually. As a result, they may not be as bound by the internal professional norms, ethical frameworks, or institutional logic that shape the decision-making of career defense, intelligence, and diplomatic officials. While they are undoubtedly part of a global professional elite, their priorities differ from those of individuals who have spent their entire careers in government service within the national security and foreign policy spheres.[264]

Most importantly, the primary mission of tech giants is not to advance the national security interests of their home countries and, in some cases, their employees have explicitly resisted involvement in military or defense-related operations.[265] By design, their fundamental objective is profitability, and their market incentives push them to develop secure, high-quality products that maintain consumer trust—was made evident in the emphasis on Apple's product security in its complaint against NSO.[266] While tech giants may be receptive to certain national security considerations and, in some cases, willing to tolerate limited privacy intrusions, they are less inclined to prioritize government interests over user protections compared to state security agencies which are, ultimately, a component part of the executive branch.

Further, tech giants are less constrained by jurisdictional limitations, at least so long as the doctrinal framework established in *WhatsApp v. NSO* remains intact.[267] In their complaints against NSO, both Apple and WhatsApp explicitly argued that American courts have jurisdiction over cases involving commercial

---

[264] Aziz Rana, *Who Decides on Security?*, 44(5) CONN. L. REV., 1417, 1486-90 (2012).
[265] E.g.: Karp & Zamiska, *supra* note 261, 33-35.
[266] Apple's Complaint, *supra* note 195.
[267] Order re Mot. for Summ. J., WhatsApp Inc. v. NSO Grp. Techs., Ltd., No. 4:19-cv-07123 (N.D. Cal. Dec. 20, 2024).

spyware firms because the targeted servers are located on U.S. soil. Apple, for instance, asserted that "[NSO would …] send abusive data . . . through Apple servers in the United States and abroad for purposes of attack."[268] In *WhatsApp*, the district court affirmed a similar reasoning, recognizing that: "[NSO] caused a digital transmission to enter California, which then effectuated a breaking and entering of a server in California. Accordingly, the court finds that the evidentiary record supports the conclusion that defendants are subject to personal jurisdiction in this district."[269]

In other words, the jurisdictional challenges that state-sponsored regulatory agencies face do not arise in the context of litigation initiated by tech giants with (key) infrastructure in the United States. What matters for them is neither where the software is developed, nor where the attacked device has been located. As long as the servers operated by the tech giants are located in the United States and are subject to attack, jurisdiction may be established, regardless of where the spyware company operates. For Pegasus to function, it must necessarily compromise servers, even if the ultimate target is located outside the United States. This principle, as explained in *WhatsApp v. NSO*, highlights the distinction: while spyware firms may relocate across jurisdictions to evade state-sponsored regulation on defense export, such maneuvers do not seem to shield them from liability in U.S. courts.

Finally, tech giants are better positioned than state-sponsored, defense-oriented agencies in terms of both resources and expertise to engage in this form of de facto regulation. Effective litigation requires access to technical evidence regarding how servers have been attacked. In *WhatsApp v. NSO*, for instance, WhatsApp was able to present the court with detailed forensic evidence demonstrating how its servers were infiltrated by Pegasus.[270] By design, tech giants also employ highly skilled security professionals dedicated to securing their products. They possess not only the financial means to sustain prolonged legal battles but also the technical expertise to diagnose and analyze commercial spyware operations. As a result, tech giants are uniquely equipped

---

[268] Apple's Complaint, *supra* note 195, at 14.
[269] Order re Mot. for Summ. J., WhatsApp v. NSO Grp., *supra* note 7, at 6.
[270] WhatsApp's Complaint, *supra* note 206.

to pursue litigation against spyware firms, in contrast to agencies like DECA, which may lack the cybersecurity expertise or at least the capacity to conduct sophisticated technical assessments of spyware capabilities.

b) In Comparison with Individual Plaintiffs

Although American courts have found Israel to be the appropriate forum when individuals sued NSO in the United States, litigation in Israel has been largely unsuccessful thus far. Since legal proceedings concerning NSO in Israel are conducted largely in secrecy and subject to gag orders, the precise reasons for this situation remain unclear. However, interviews with attorneys involved in these cases suggest that the Israeli legal system has imposed significant restrictions on plaintiffs' ability to proceed beyond discovery. Moreover, jurisdictional challenges were also raised in Israeli courts, potentially mirroring the barriers plaintiffs faced in the United States.[271]

This pattern may raise questions about whether the doctrine of forum non conveniens should, in fact, bar litigation by individual plaintiffs in U.S. courts. But it also underscores a broader structural challenge: individuals face substantial barriers when attempting to litigate against spyware firms. Individuals directly harmed by commercial spyware often struggle to secure a viable forum for litigation, rendering such lawsuits lengthy, costly, and practically difficult to sustain. These barriers, in turn, effectively limit their ability to hold spyware firms accountable. In other words, this Article shows that there are potentially plausible arguments against dismissing individual plaintiffs' cases on forum non conveniens grounds, given the apparent lack of practical ability to litigate effectively in Israel. It does not advance that claim definitively, however, because much of the relevant litigation in Israel remains sealed and, in certain cases, ongoing. Nor is it clear that the Israeli legal system, even if unfavorable to individual plaintiffs in this context, is categorically incapable of granting any remedy at all. Still, even if individual plaintiffs succeed in overcoming the jurisdictional barrier, they are likely to face severe practical

---

[271] Interview with Alaa Mahajna, *supra* note 177; Interview with Eitay Mack, *supra* note 168.

obstacles in litigating against spyware firms without the support of larger organizations, whether Big Tech companies, NGOs, or other institutional actors.

As the *WhatsApp* case demonstrates, to begin with, tech giants do not face the same jurisdictional hurdles that have consistently limited litigation brought by individuals. Even when they are faced with jurisdictional challenges, they obviously have more resources to invest in the litigation.

In *WhatsApp v. NSO*, the court found that personal jurisdiction over NSO in the United States was proper because WhatsApp was able to demonstrate that its U.S.-based servers had been compromised as part of the attack.[272] This finding was based on a technical demonstration of how the exploit functioned, which WhatsApp presented as evidence in the case. Individual plaintiffs lack this advantage. Without direct access to the technical architecture of Pegasus or concrete evidence regarding how the malware operated in their specific instances, individual plaintiffs are at a disadvantage when attempting to establish jurisdiction. Tech giants, by contrast, are far better positioned to overcome these jurisdictional barriers, as they possess the necessary evidence to prove where and how their servers were attacked.

This evidentiary advantage also highlights another key reason why tech giants are more effective litigants against commercial spyware firms: their superior access to information. Individual plaintiffs, such as Corallo, must rely on speculation when attempting to establish personal jurisdiction. In *Corallo*, for example, the court explicitly noted that "Corallo's insistence that NSO targeted Apple's servers in California is not only speculative as a factual matter, but legally insufficient to give rise to personal jurisdiction over NSO."[273] Unlike tech giants, private plaintiffs do not have access to data or internal records regarding how Pegasus exploited digital infrastructure. The best they can do is rely on third-party technical reports from independent organizations such as Citizen Lab, evidence that courts have found insufficient for establishing jurisdiction.[274]

---

[272] Order re Mot. for Summ. J., WhatsApp v. NSO Grp., *supra* note 7.
[273] Order re Mot. to Dismiss, Corallo v. NSO Grp., *supra* note 108, at 6.
[274] *E.g.*, The Citizen Lab, *supra* note 13; The Citizen Lab, *supra* note 74.

Moreover, tech giants are unlikely to share this information with individual plaintiffs, as the *Apple v. NSO* case may suggest. Despite initiating litigation against NSO, Apple ultimately voluntarily dismissed its own lawsuit in order to avoid disclosing sensitive information.[275] However, when tech giants choose to pursue litigation, they have direct access to critical technical evidence and are able to present it effectively, as WhatsApp's complaint demonstrated.[276]

Beyond these advantages, tech giants are generally "haves"—actors with resources and the tendency to be repeat-players—while individual plaintiffs are more accurately classified as "have-nots," using Galanter's theoretical framework for the social analysis of litigation.[277] In other words, tech giants enjoy institutional advantages in litigation, both in terms of having more resources, more familiarity with the proceedings, and the ability to "play for the rule" and not for the case. In an interview, Adv. Mahajna emphasized that, in his experience, individuals simply do not have the financial resources or capacity to pursue this kind of litigation due to its cost and the time investment required.[278] This reality exemplifies Galanter's theory application: tech giants are structurally better positioned to engage in litigation.

As Galanter famously observed, the advantages of repeat players (RPs) extend far beyond financial wealth. While RPs are often wealthier than one-shotters (OSs), their additional advantages lie in their familiarity with the legal system and their ability to engage in long-term legal strategy, playing for the rule rather than the case.[279] For example, RPs can develop institutional relationships with courts, fostering a level of credibility that individual plaintiffs lack.[280] More importantly, they litigate not merely for case-specific circumstances, but to shape legal doctrine. Individual plaintiffs, such as Corallo, the *Dada* plaintiffs, or Jamal Khashoggi's widow, can focus exclusively on the specific human rights violations they suffered. They seek redress for their personal damages, but they

---

[275] Apple's Mot. to Dismiss, *supra* note 115, at 2.
[276] WhatsApp's Complaint, *supra* note 206.
[277] Marc Galanter, *Why the 'Haves' Come out Ahead: Speculation on the Limits of Legal Change*, 9(1) LAW & SOC'Y REV. 95 (1974).
[278] Interview with Alaa Mahajna, *supra* note 177.
[279] Galanter, *supra* note 277, at 100.
[280] *Id.* at 99.

often may lack the legal incentive or institutional capacity to litigate for broader doctrinal change that would prevent future abuses.

Tech giants, by contrast, are invested in deterring spyware firms from attacking their products in the future. Their primary concern is not the specific privacy violation at issue in a given case; the exploited vulnerability in question has typically long been fixed by the time litigation is initiated.[281] Instead, they are concerned with the legal precedent set by the litigation, ensuring that commercial spyware firms face real consequences for their actions. This broader strategic interest enables them to litigate cases to the fullest extent, making it far less likely that a spyware firm could neutralize a lawsuit with a confidential settlement, for example. If liability is established, a tech giant has much less of an incentive to settle quietly, as its goal may be regulatory deterrence. Thus, their status as RPs, rather than OSs, affords them yet another structural advantage in this form of litigation.

Lastly, as the district's ruling in *WhatsApp v. NSO* demonstrated, tech giants can be at least partially successful at obtaining injunction orders limiting commercial spyware firms' operations, under the CFAA.[282] The district court in *WhatsApp* granted an injunction, excluding sovereign governments from its scope and narrowing it only to WhatsApp's platform itself, and thereby limiting NSO's ability to attack WhatsApp's servers in the future.[283] NSO argued strongly against and asked to stay the injunction, despite the reduced compensation, suggesting that the injunction itself is harmful for the spyware firm.[284] Although the injunction was narrowed to apply only to WhatsApp's platform—and not Meta's other platforms—the plaintiffs, through this injuunction were nonetheless able to protect an entire platform. In this regard, they may have another advantage over individuals, who can only protect themselves, and not other users of the platform through which they were targeted. For this reason,

---

[281] *E.g.*, Miles Kenyon, *WhatsApp Rushes to Fix Security Flaw Exposed in Hacking of Lawyer's Phone*, THE CITIZEN LAB (May 13, 2019), www.citizenlab.ca/2019/05/whatsapp-voice-calls-used-to-inject-nso-group-spyware-in-phones.
[282] 18 U.S.C. § 1030.
[283] Order re Mot. for Perm. Inj., WhatsApp v. NSO, *supra* note 222.
[284] Reply in Support of Mot. to Stay Perm. Inj., WhatsApp v. NSO, *supra* note 227.

too, tech giants are uniquely positioned to mitigate the harms caused by spyware vendors.

2. Incentives

The ability to litigate against spyware firms does not necessarily translate into a willingness to do so. State regulators have a legal mandate to oversee defense exports. Individual plaintiffs have a personal stake in seeking redress. What could drive tech giants to litigate these cases?

A useful starting point for this analysis is Alan Rozenshtein's framework of tech giants as "surveillance intermediaries."[285] Rozenshtein argues that while tech giants play a crucial role in enabling state surveillance, they differ from historical equivalents, in that they are less willing to cooperate (almost) unconditionally. Instead, they often position themselves as intermediaries that mitigate the power of the "surveillance executive."[286]

Rozenshtein identifies both financial and ideological incentives that drive this behavior. Financially, tech giants have recognized that resisting surveillance and enhancing the security of their products can serve as a form of product differentiation.[287] A reputation for strong privacy protections can increase consumer trust and boost competitiveness.[288] Ideologically, tech giants may be influenced by what scholars have referred to as the "Californian Ideology," a worldview that opposes excessive government surveillance and may even often align with libertarian principles.[289] These financial and ideological incentives may also explain why tech giants would be motivated to challenge commercial spyware firms through litigation. By doing so, they reinforce their market position as defenders of user privacy while simultaneously curbing the proliferation of tools that could undermine their products' security.

---

[285] Rozenshtein, *supra* note 6.
[286] *Id.* at 104; BRIAN HOCHMAN, THE LISTENERS: A HISTORY OF WIRETAPPING IN THE UNITED STATES 220-40 (2022).
[287] Rozenshtein, *supra* note 285, 116.
[288] *Id.* at 116-17.
[289] *Id.* at 118.

Tech giants employ various "techniques of resistance" to limit government surveillance, including technological unilateralism, policy mobilization, and, most relevant to this context, proceduralism and litigiousness.[290] This analysis primarily focuses on the direct interactions between tech giants and law enforcement, such as when authorities request access to user data.[291]

Applying this framework to the regulation of commercial spyware, the same incentives may also motivate tech giants to challenge spyware firms through litigation. As Davidson phrased it: "Big Tech is involved not only in protecting targets and reinforcing the security of its own products, but in norm development, diffusion and enforcement, as well as efforts to shape the regulatory landscape […] *the regulation of spyware is a new stage in Big Tech's involvement in geopolitical conflict, human rights and cyber security, which until now has included standard-setting* and the enforcement of rights."[292]

The key difference between the position tech giants occupy when they receive direct government requests for cooperation and the position they occupy when their products are targeted by commercial spyware is that, in the latter context, they are not responding to government demands, but rather are left out of the loop. Commercial spyware enables governments to obtain access to user data, devices, and communications while circumventing the procedural requirements that would ordinarily apply when law enforcement agencies request information directly from technology companies. In this regard, commercial spyware sidelines tech giants and renders their policies largely irrelevant: they are not parties to the decisions to surveil users or gain access to users' data. Technology companies therefore have an interest in ensuring that these tools are subject to strict regulation, among other reasons, in order to preserve their own powers.

First, as outlined in the *WhatsApp* complaint, commercial spyware such as Pegasus directly compromises the servers of tech giants, exploiting their

---

[290] *Id.* at 122-44.
[291] *Id.* at 123.
[292] Davidson, *supra* note 5, at 481.

infrastructure to facilitate unauthorized intrusions into user devices.[293] In essence, the very existence of these spyware tools depends on their ability to manipulate the technological infrastructure of major platforms. This unauthorized use of tech giants' property undermines these companies' security frameworks and exposes them to significant potential operational and reputational costs.

Moreover, the presence of commercial spyware creates an ongoing arms race between spyware firms and tech companies. Spyware developers continually seek new vulnerabilities to exploit and sell, while tech giants must invest substantial resources into identifying and patching these weaknesses. This dynamic imposes significant financial and technical burdens on tech companies, as they are forced to devote funds and personnel to securing their platforms against an evolving, shape-shifting threat. Limiting the activities of commercial spyware firms through litigation, therefore, aligns with tech giants' financial interests, because reducing the capabilities and attractiveness of such spyware reduces the costs associated with this security race. Another related point, mentioned by Davidson, is that Big Tech's business model is built on mass surveillance, and restraining the development of the spyware market in this regard financially aligns with Big Tech's interest in maintaining dominance over surveillance practices.[294]

Second, tech giants may struggle to maintain consumer trust and market dominance if their products are compromised by commercial spyware. Privacy and cybersecurity are central concerns for at least some users. For certain companies, security is a defining aspect of their brand identity and product differentiation. A reputational concern is likely one of the driving forces behind the litigation against NSO, as evident in Apple's complaint.[295] Both Apple and

---

[293] WhatsApp's Complaint, *supra* note 206.
[294] Davidson, *supra* note 5, at 528.
[295] Apple's Complaint, *supra* note 195.

WhatsApp, for example, emphasize the strength of their encryption and their commitment to user privacy.[296]

In other words, unlike individual plaintiffs, who primarily seek redress for specific harms, tech companies have a long-term strategic interest in deterring spyware firms from engaging in future attacks. If spyware firms remain undeterred, tech companies will continue to face an escalating cybersecurity arms race, requiring ever-greater investments in vulnerability research and mitigation strategies. This dynamic provides a strong financial and strategic incentive for tech giants to engage in litigation as a means of regulating commercial spyware.

A third incentive for technology companies to engage in litigation against commercial spyware firms is, essentially, public relations. These companies seek to sell their products, and a central component of their marketing strategy could be the claim that their platforms are secure, reliable, and worthy of user trust. Beyond that, it is a source of their legitimacy. As Davidson writes, "Big Tech's discourse contrasting itself with spyware companies and applauding itself for being a champion of privacy, human rights, and democracy, suggests that the regulation of spyware also serves as one of the avenues through which Big Tech legitimates itself . . . in the case of Big Tech, the need for legitimation is especially strong given the growing dependence of states on Big Tech."[297] Litigation, then, provides technology companies with an opportunity to reinforce this narrative by demonstrating that they take cybersecurity threats seriously and are actively working to protect users from malicious actors, especially because such lawsuits often attract substantial press coverage.[298] For

---

[296] *E.g.*, *Privacy*, APPLE.COM (last visited Dec. 15, 2025), https://perma.cc/U7Y2-WRZ9; *Messaging Privately*, WHATSAPP.COM (last visited Dec. 15, 2025), https://perma.cc/YN9M-EV6M.

[297] Davidson, *supra* note 5, at 530.

[298] E.g., Nicole Perlroth, WhatsApp Says Israeli Firm Used Its App in Spy Program, N.Y. TIMES (Oct. 29, 2019), https://perma.cc/6BGY-AZRE; Reuters Staff, US judge finds Israel's NSO Group liable for hacking in WhatsApp lawsuit, REUTERS (Dec. 23, 2024), www.reuters.com/technology/cybersecurity/us-judge-finds-israels-nso-group-liable-hacking-whatsapp-lawsuit-2024-12-21; Blake Montgomery, US judge finds Pegasus spyware maker liable over WhatsApp hack, THE GUARDIAN (Dec. 20, 2024), https://perma.cc/2EZ9-7EZ6.

Big Tech, serving, or at least being perceived as serving, as a de facto regulator in this space can therefore contribute to public legitimacy.

However, as discussed above, these incentives persist only so long as the financial, ideological, and reputational incentives that support them remain in place.[299] If public concern for privacy, due process, and related rights fades, and if Rozenshtein's "Californian ideology"[300] likewise weakens, Big Tech companies may become more strongly incentivized to align with government requests or with the national security apparatus than to resist the commercial spyware industry. Under those conditions, much of the analysis presented here could quickly become obsolete, and the public would lose yet another potential regulatory actor in the field of commercial spyware. Technology companies can serve as a complementary regulatory mechanism, but they are not designed to be the only actors in this field.

This Article thus presents both a promise and a warning. The promise lies in the emerging role of litigation as a complementary regulatory mechanism in the commercial spyware domain, especially when such litigation is initiated or supported by institutionally powerful actors, first and foremost technology companies. Big Tech companies do have incentives to play that role, but they also face meaningful counterincentives. The public, civil society, and even privacy-enhancing political actors therefore have an important role to play in ensuring that technology companies remain incentivized not to become fully embedded within the national security apparatus, but instead to remain independent actors capable of challenging commercial spyware firms when public interests so require.

CONCLUSION

Traditional regulatory mechanisms appear to have failed to constrain human rights abuses by commercial spyware.[301] Faced with this regulatory

---

[299] Rozenshtein, supra note 6, at 118.
[300] Id.
[301] Lubin, *supra* note 4.

gap,[302] individuals targeted by these tools have sometimes turned to litigation in U.S. courts in search of accountability. Based on this Article's examination of NSO Group and its Pegasus spyware as a case study, however, those efforts have thus far fallen short of achieving the plaintiffs' goals. U.S. courts have dismissed suits brought by individual plaintiffs on jurisdictional and forum non conveniens grounds, directing plaintiffs to Israel as an alternative forum.

Yet, as demonstrated through docket analysis and interviews with the attorneys involved, litigation in Israel has thus far provided little meaningful redress. This experience suggests that, at least in the context of NSO, individual litigation faces serious structural and practical obstacles that limit its capacity to function as an effective accountability mechanism for commercial spyware abuses.

Building on the emerging body of literature identifying Big Tech's emerging role as a "surveillance intermediary" generally [303] and particularly in the commercial spyware context,[304] this Article argues that litigation initiated or backed by major technology companies can serve a distinct and increasingly important regulatory function. Unlike state regulators, technology companies are not institutionally bound to prioritize national security or diplomatic interests over other considerations. Unlike individual plaintiffs, they possess the resources, technical expertise, evidentiary access, and legal standing necessary to pursue complex, transnational litigation. The litigation brought by WhatsApp against NSO illustrates this difference. There, a U.S. court found NSO liable and imposed injunctive relief limiting NSO's operations. Even though the remedies were narrowed, the case demonstrates that technology companies may succeed where individual plaintiffs and regulators have not.

The Article situates this discussion within a broader theory of litigation power. Individual victims of spyware abuse are classic one-shot litigants: their claims are retroactive, anecdotal, and resource-constrained. Technology companies, by contrast, are repeat players. Their interest lies not in a particular

---

[302] Davidson, *supra* note 5, at 480-81.
[303] Rozenshtein, *supra* note 6.
[304] Davidson, *supra* note 5.

vulnerability or past intrusion, but in shaping legal rules that alter the underlying incentives of the spyware market itself. By litigating for precedent rather than settlement, and for deterrence rather than individualized relief, these firms can effectively operate as de facto regulators. Drawing on comprehensive docket analysis and original interviews, this Article demonstrates that litigation initiated by technology companies can function as a meaningful, though limited, regulatory mechanism in a domain where existing oversight is structurally constrained. Under current institutional conditions, such litigation may represent a viable pathway for imposing legally significant constraints on commercial spyware vendors and for promoting accountability in an otherwise underregulated surveillance market.