2022,[22] just before the opening of the HRC's forty-ninth session, scheduled from February 20 to April 1.[23] In remarks to the Council on March 1, Blinken condemned Russia's invasion of Ukraine and praised the Council's "decision to hold an urgent debate on the crisis," while also highlighting other areas "where the Council's attention is needed," including Belarus, China, and Afghanistan.[24] Blinken further pledged that the United States will focus on strengthening economic, social, and cultural rights as well as civil and political rights, work to "counter anti-Israel bias," and "keep fighting for the human rights of LGBTQI+ people; people with disabilities; members of racial, ethnic, and religious minorities; women and girls; and all marginalized populations and people in vulnerable situations."[25]

International Economic Law

United States Makes Efforts to Curb Misuse of Surveillance Technology

doi:10.1017/ajil.2022.13

In November 2021, following numerous reports of misuse, the Biden administration placed surveillance technology companies—including the Israeli firm NSO Group—on the Commerce Department's Entity List,[1] a designation that "prohibits export from the United States to NSO of any type of hardware or software, severing the company from a vital source of technology."[2] So-called "spyware," such as the NSO Group's Pegasus software, is used to hack into mobile devices, "secretly harvest[ing] all of the data on a phone and deploy[ing] the microphone and camera."[3] Although surveillance technology companies assert that they sell software to governments for use in criminal and terrorism investigations, investigative reporting has revealed numerous instances of misuse of surveillance technology to spy on journalists, lawyers, and activists, among others. WhatsApp and Apple have sued NSO Group in U.S. federal court for exploiting their platforms to spy on users, and through measures like the Entity List, the Biden administration is attempting to curb the misuse of surveillance technology. Congress has also taken steps to restrict the use of spyware, including

[22] PN1296 - Nomination of Michele Taylor for Department of State, 117th Congress (2021–2022), PN1296, 117th Cong. (2022), *at* https://www.congress.gov/nomination/117th-congress/1296.

[23] Human Rights Council, Agenda and Annotations, UN Doc. A/HRC/49/1 (Jan. 17, 2022), *at* https://undocs.org/A/HRC/49/1.

[24] U.S. Dep't of State Press Release, Remarks at the UN Human Rights Council 49th Session (Mar. 1, 2022), *at* https://www.state.gov/remarks-at-the-un-human-rights-council-49th-session [https://perma.cc/656C-V5FG].

[25] *Id.*

[1] U.S. Dep't of Commerce Press Release, Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021), *at* https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list [https://perma.cc/SC22-D2XM].

[2] Drew Harwell, Ellen Nakashima & Craig Timberg, *Biden Administration Blacklists NSO Group Over Pegasus Spyware*, Wash. Post (Nov. 3, 2021), *at* https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware.

[3] Julie Bloch, Sukti Dhital, Rashmika Nedungadi & Nikki Reisch, *CTRL+HALT+Defeat: State-Sponsored Surveillance and the Suppression of Dissent*, Just Security (May 15, 2019), *at* https://www.justsecurity.org/64095/ctrlhaltdefeat-state-sponsored-surveillance-and-the-suppression-of-dissent.

by requiring the secretary of defense, in consultation with the director of national intelligence and other federal agencies as appropriate, to report to Congress a list of companies that sell surveillance technology that has been misused. Challenges, however, remain as new companies exploit a burgeoning market for surveillance technology.

At the center of the growing concern surrounding surveillance technology is NSO Group, an Israeli company that sells the Pegasus surveillance software. NSO markets Pegasus as a tool that "helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe."[4] NSO asserts that its technology is "used exclusively by government intelligence and law enforcement agencies."[5] In certain cases, the technology appears to have done what NSO Group advertises. Mexican law enforcement reportedly used the surveillance technology during the operation to capture and arrest Joaquín Guzmán Loera, the drug cartel leader known as "El Chapo."[6] In another instance, the software reportedly helped European law enforcement "take down a global child-abuse ring."[7]

But a number of investigations by academic institutes and the media have revealed that NSO's Pegasus software has been used to target dissidents and government officials, among others. Two early revelations about misuse came in 2016 and 2017. In 2016, the University of Toronto's Citizen Lab published a report detailing its investigation into the United Arab Emirates' use of Pegasus to surveil Ahmed Mansoor, "an internationally recognized human rights defender."[8] In 2017, a *New York Times* investigation revealed that the Mexican government used Pegasus against "human rights lawyers, journalists and anticorruption activists."[9] Then in 2021, the Pegasus Project, an international, collaborative investigation into the misuse of NSO Group's surveillance technology in which seventeen media organizations participated,[10] uncovered a list of more than 50,000 phone numbers, located in over fifty countries, that may have been targeted by Pegasus.[11] The investigative team also confirmed dozens of smartphone hacks, including on the phones of murdered Saudi journalist Jamal Khashoggi's wife and fiancée[12] and of dissidents in Poland and Hungary.[13] The database even included French President Emmanuel Macron's phone number.[14] Although NSO Group has repeatedly asserted that "'[i]t is technologically impossible'" for

[4] NSO Group, *at* https://www.nsogroup.com.

[5] NSO Group, *About Us*, *at* https://www.nsogroup.com/about-us.

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

[7] *Id.*

[8] Bill Marczak & John Scott-Railton, *The Million Dollar Dissident*, Citizen Lab (Aug. 24, 2016), *at* https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae.

[9] Azam Ahmed & Nicole Perlroth, *Using Texts as Lures, Government Spyware Targets Mexican Journalists and Their Families*, N.Y. Times (June 19, 2017), *at* https://www.nytimes.com/2017/06/19/world/americas/mexico-spyware-anticrime.html.

[10] Forbidden Stories, *About the Pegasus Project*, *at* https://forbiddenstories.org/about-the-pegasus-project.

[11] Dana Priest, Craig Timberg & Souad Mekhennet, *Private Israeli Spyware Used to Hack Cellphones of Journalists, Activists Worldwide*, Wash. Post (July 18, 2021), *at* https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones.

[12] Dana Priest, Souad Mekhennet & Arthur Bouvart, *Jamal Khashoggi's Wife Targeted With Spyware Before His Death*, Wash. Post (July 18, 2021), *at* https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack.

[13] Daniel Boffey, *EU to Launch Rare Inquiry Into Pegasus Spyware Scandal*, Guardian (Feb. 10, 2022), *at* https://www.theguardian.com/news/2022/feb/10/eu-close-to-launching-committee-of-inquiry-into-pegasus-spyware.

[14] *Id.*

https://doi.org/10.1017/ajil.2022.13 Published online by Cambridge University Press

Pegasus to be deployed against phones with a U.S. +1 number or phones in the United States,[15] in December 2021 news broke of "the first confirmed cases of Pegasus being used to target American officials," namely U.S. embassy staff in Uganda.[16]

Following these reports of misuse, the messaging platform WhatsApp and its parent company Facebook (now Meta) sued NSO Group in U.S. federal court in California in October 2019. The complaint alleges that NSO Group "reverse-engineered the WhatsApp app and developed a program to enable them to emulate legitimate WhatsApp network traffic in order to transmit malicious code—undetected—to Target Devices over WhatsApp servers," ultimately targeting roughly 1,400 devices used by "attorneys, journalists, human rights activists, political dissidents, diplomats, and other senior foreign government officials."[17] WhatsApp seeks "injunctive relief and damages pursuant to the Computer Fraud and Abuse Act . . . and the California Comprehensive Computer Data Access and Fraud Act" as well as pursuant to "breach of contract and trespass to chattels" claims.[18] NSO Group moved to dismiss for a lack of subject matter jurisdiction, arguing that "conduct giving rise to the complaint was performed by foreign sovereigns and the Foreign Sovereign Immunit[ies] Act ('FSIA') . . . bars any lawsuit" on the basis of foreign sovereigns' or their contractors' conduct.[19] The district court denied NSO Group's motion to dismiss,[20] and NSO appealed.[21]

On November 8, 2021, the Ninth Circuit affirmed the district court's decision, unanimously denying NSO's motion to dismiss and rejecting its attempt to claim immunity. The court recognized that

> [n]either the Supreme Court nor this Court has answered whether an entity that does not qualify as a "foreign state" can claim foreign sovereign immunity under the common law. It is clear under existing precedent that such an entity cannot seek immunity under the FSIA. Whether such entity can sidestep the FSIA hinges on whether the Act took the entire field of foreign sovereign immunity as applied *to entities*, or whether it took the field only as applied to foreign *state* entities, as NSO suggests.[22]

The court determined that "an entity is entitled to foreign sovereign immunity, if at all, only under the FSIA. If an entity does not fall within the Act's definition of 'foreign state,' it cannot claim foreign sovereign immunity. Period."[23] The court explained that "the omission of entities like NSO from the FSIA's definition of foreign states and their 'political subdivisions,

[15] Craig Timberg, John Hudson & Kristof Clerix, *Key Question for Americans Overseas: Can Their Phones Be Hacked?*, WASH. POST (July 19, 2021), *at* https://www.washingtonpost.com/national-security/2021/07/19/us-phone-numbers-nso.

[16] Craig Timberg, Drew Harwell & Ellen Nakashima, *Pegasus Spyware Used to Hack U.S. Diplomats Working Abroad*, WASH. POST (Dec. 3, 2021), *at* https://www.washingtonpost.com/technology/2021/12/03/israel-nso-pegasus-hack-us-diplomats.

[17] Complaint at 8–9, WhatsApp Inc. et al. v. NSO Group Techs. Ltd. et al., No. 3:19-cv-07123 (N.D. Cal. Oct. 29, 2019) (Doc. 1).

[18] *Id.* at 2.

[19] WhatsApp Inc. v. NSO Group Techs. Ltd., 472 F. Supp. 3d 649, 663 (N.D. Cal. 2020).

[20] *Id.* at 667.

[21] Notice of Appeal, WhatsApp Inc. et al. v. NSO Group Techs. Ltd. et al., No. 4:19-cv-07123-PJH (N.D. Cal. July 21, 2020) (Doc. 112).

[22] WhatsApp Inc. v. NSO Group Techs. Ltd., 17 F.4th 930, 937 (9th Cir. 2021).

[23] *Id.*

https://doi.org/10.1017/ajil.2022.13 Published online by Cambridge University Press

agencies, and instrumentalities' reflects a threshold determination about the availability of foreign sovereign immunity for such entities: they never qualify."[24] The court further explained that there was no need to examine whether NSO is entitled to foreign official immunity under the common law, but noted the "compelling fact" that "neither the State Department nor any court has ever applied foreign official immunity to a foreign private corporation under the common law."[25] The court therefore affirmed the district court's denial of NSO's motion to dismiss.[26] The Ninth Circuit denied rehearing and rehearing en banc,[27] and NSO has filed a petition for certiorari with the Supreme Court.[28]

WhatsApp's suit is not the only civil claim against NSO. In November 2021, Apple sued NSO, seeking "a permanent injunction to ban NSO Group from using any Apple software, services, or devices."[29] Apple alleged NSO Group violated the Computer Fraud and Abuse Act and the California Business and Professions Code by selling what Citizen Lab dubbed the FORCEDENTRY spyware and allowing clients to hack into Apple users' devices.[30] In order to hack into Apple devices, NSO engineers had to create Apple IDs and agree to Apple's terms and conditions, which contain a clause subjecting users to the laws of California—thereby giving Apple a cause of action against NSO.[31] Apple executives framed the case "as a warning shot to NSO and other spyware makers" that attempt to deploy spyware on Apple devices, with one explaining, "'If you do this, if you weaponize our software against innocent users, researchers, dissidents, activists or journalists, Apple will give you no quarter.'"[32]

In the biggest move against surveillance tech to date, the U.S. government added NSO Group and another Israeli surveillance technology firm, Candiru, to the Entity List on November 3.[33] The Commerce Department explained that

> NSO Group and Candiru (Israel) were added to the Entity List based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers. These tools have also enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments

[24] *Id.* at 939.

[25] *Id.* at 940.

[26] *Id.*

[27] Order, WhatsApp, LLC et al. v. NSO Group Techs. Ltd. et al., No. 20-16408 (9th Cir. Jan. 6, 2022); *see also* Andrea Vittorio, *NSO Loses Latest Challenge to Meta Lawsuit Over WhatsApp Spyware*, Bloomberg Law (Jan. 6, 2022), *at* https://news.bloomberglaw.com/privacy-and-data-security/nso-loses-latest-challenge-to-meta-lawsuit-over-whatsapp-spyware.

[28] Josef Federman, *NSO Turns to US Supreme Court for Immunity in WhatsApp Suit*, Assoc. Press (Apr. 11, 2022), *at* https://apnews.com/article/us-supreme-court-technology-business-spyware-lawsuits-3a2cdcfdac224647bd65e95fd57395d5.

[29] *Apple Sues NSO Group to Curb the Abuse of State-Sponsored Spyware*, Apple (Nov. 23, 2021), *at* https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware.

[30] *See* Complaint, Apple Inc. v. NSO Group Techs. Ltd. et al., No. 5:21-cv-09078 (N.D. Cal. Nov. 23, 2021) (Doc. 1).

[31] Nicole Perlroth, *Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones*, N.Y. Times (Nov. 23, 2021), *at* https://www.nytimes.com/2021/11/23/technology/apple-nso-group-lawsuit.html.

[32] *Id.* (quoting Ivan Krstic, Apple's head of security engineering and architecture).

[33] U.S. Dep't of Commerce Press Release, *supra* note 1; U.S. Dep't of Commerce, Final Rule, Addition of Certain Entities to the Entity List, 86 Fed. Reg. 60,759 (Nov. 4, 2021) [hereinafter Commerce Dep't Final Rule].

https://doi.org/10.1017/ajil.2022.13 Published online by Cambridge University Press

> targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order.[34]

Inclusion on the Entity List "restrict[s] the export, reexport, and in-country transfer of items subject to" export controls to listed companies.[35] To transfer export controlled items to listed entities requires a license, and the Commerce Department determined that as to NSO and Candiru, there should be a presumption of denial of license requests and no exceptions to the license requirement.[36]

While the United States has included companies like China's Huawei on the Entity List,[37] media reports expressed surprise at the listing of a company with ties to a close U.S. ally, characterizing the move as a "remarkable breach with Israel."[38] NSO Group's sales are subject to Israeli government review pursuant to export controls.[39] When the news of Pegasus misuse broke over the summer, Israel's defense ministry stated that it would revoke export licenses for Israeli surveillance technology companies if there were any "contravention of the terms of the license, especially after any violation of human rights,"[40] but the *New York Times* reported that Israel issued new licenses, including to NSO, to export to Saudi Arabia after the role of Pegasus in Saudi Arabia's state-sponsored murder of Jamal Khashoggi came to light.[41] Israeli officials reacted negatively to the listing of NSO Group and Candiru. According to reports, the United States informed Israel's Ministry of Defense "less than an hour before it was made public"—a move that made Israeli officials "furious."[42] The State Department, however, noted that the Biden administration is not "taking action against countries . . . where these entities are located."[43]

The Entity List additions build on other executive branch actions to address surveillance tech. In October, the Commerce Department released an interim final rule aimed at limiting the spread of "items that can be used for malicious cyber activities" and "ensur[ing] that U.S. companies are not fueling authoritarian practices."[44] The rule, which would cover, among other things, Pegasus, "will align the United States with the 42 European and other allies

[34] U.S. Dep't of Commerce Press Release, *supra* note 1.

[35] *Id.*

[36] Commerce Dep't Final Rule, *supra* note 33.

[37] *Commerce Adds Huawei Technologies Co. Ltd. to the Entity List*, BLOOMBERG (May 15, 2019), *at* https://www.bloomberg.com/press-releases/2019-05-15/commerce-adds-huawei-technologies-co-ltd-to-the-entity-list.

[38] David E. Sanger, Nicole Perlroth, Ana Swanson & Ronen Bergman, *U.S. Blacklists Israeli Firm NSO Group Over Spyware*, N.Y. TIMES (Nov. 3, 2021), *at* https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html.

[39] Peter Beaumont & Philip Oltermann, *Israel to Examine Whether Spyware Export Rules Should Be Tightened*, GUARDIAN (July 22, 2021), *at* https://www.theguardian.com/news/2021/jul/22/israel-examine-spyware-export-rules-should-be-tightened-nso-group-pegasus.

[40] Ronen Bergman & Mark Mazzetti, *Israeli Companies Aided Saudi Spying Despite Khashoggi Killing*, N.Y. TIMES (July 17, 2021), *at* https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html.

[41] *Id.*

[42] Bergman & Mazzetti, *supra* note 6.

[43] U.S. Dep't of State Press Release, The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities (Nov. 3, 2021), *at* https://www.state.gov/the-united-states-adds-foreign-companies-to-entity-list-for-malicious-cyber-activities [https://perma.cc/5LA8-DRNN].

[44] U.S. Dep't of Commerce Press Release, Commerce Tightens Export Controls on Items Used in Surveillance of Private Citizens and Other Malicious Cyber Activities (Oct. 20, 2021), *at* https://www.commerce.gov/news/press-releases/2021/10/commerce-tightens-export-controls-items-used-surveillance-private [https://perma.cc/

https://doi.org/10.1017/ajil.2022.13 Published online by Cambridge University Press

that are members of the Wassenaar Arrangement, which sets voluntary export control policies on military and dual-use technologies."[45] The rule imposes "a license requirement for exports to countries of national security or weapons of mass destruction concern," as well as "countries subject to a U.S. arms embargo."[46]

The Biden administration has also taken action to curb the misuse of surveillance technology by China in particular. In June, President Joseph R. Biden Jr. issued an executive order prohibiting U.S. persons from purchasing or selling "any publicly traded securities" of entities that "operate or have operated in the defense and related materiel sector or the surveillance technology sector of the economy of" China.[47] The Biden administration has designated a number of companies for involvement in the development of surveillance technology used to target the Uyghurs and other groups within China and abroad.[48]

Congress has also identified surveillance technology as a growing threat and is attempting to address misuse of such technology. In the 2022 National Defense Authorization Act, Congress included a provision that "compels the State Department to send Congress an annual report listing companies" that have used surveillance technology "directed by human rights-abusing governments."[49] In particular, it requires the Director of National Intelligence and other federal agencies to "develop or maintain . . . a list of covered contractors with respect to which the [Defense] Department should seek to avoid entering into contracts."[50] A covered contractor under this provision is one that "has knowingly assisted or facilitated a cyber attack or conducted surveillance" against the United States or a group of protected individuals like journalists and activists.[51] The Act passed the House 363–70 and the Senate 88–11,[52] and Reps. Tom Malinowski (D-NJ), Katie Porter (D-CA), Joaquin Castro (D-TX), and Anna Eshoo (D-CA) in particular called out companies that share "sensitive surveillance technology with governments in countries like Saudi Arabia, the UAE, China, or Belarus."[53]

A group of Democratic lawmakers is also pushing the Biden administration to "build on" the Entity List additions by "implement[ing] Global Magnitsky sanctions for technology companies that have enabled human rights abuses, including the arrests, disappearance,

W7L5-HAEH]; U.S. Dep't of Commerce, Interim Final Rule, Information Security Controls: Cybersecurity Items, 86 Fed. Reg. 58,205 (Oct. 21, 2021).

[45] Ellen Nakashima, *Commerce Department Announces New Rule Aimed at Stemming Sale of Hacking Tools to Russia and China*, WASH. POST (Oct. 20, 2021), *at* https://www.washingtonpost.com/national-security/commerce-department-announces-new-rule-aimed-at-stemming-sale-of-hacking-tools-to-repressive-governments/2021/10/20/ecb56428-311b-11ec-93e2-dba2c2c11851_story.html.

[46] U.S. Dep't of Commerce Press Release, *supra* note 44.

[47] Exec. Order No. 14,032, 86 Fed. Reg. 30,145 (June 7, 2021).

[48] *See* Kristen E. Eichensehr, *Contemporary Practice of the United States*, 116 AJIL 433–34 (2022).

[49] Office of Congressman Tom Malinowski Press Release, Representatives Tom Malinowski, Katie Porter, Joaquin Castro, and Anna Eshoo Applaud Congressional Passage of the "NSO Blacklist" to Counter the Hacking for Hire Industry (Dec. 16, 2021), *at* https://malinowski.house.gov/media/press-releases/representatives-tom-malinowski-katie-porter-joaquin-castro-and-anna-eshoo [https://perma.cc/S5RB-X8L9].

[50] National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, § 5502(a) (2021).

[51] *Id.* § 5502(b).

[52] *All Actions S.1605 – 117th Congress (2021–2022)*, CONGRESS.GOV, *at* https://www.congress.gov/bill/117th-congress/senate-bill/1605/all-actions?q=%7B%22roll-call-vote%22%3A%22all%22%7D&r=2&s=1&overview=closed.

[53] Office of Congressman Tom Malinowski Press Release, *supra* note 49.

https://doi.org/10.1017/ajil.2022.13 Published online by Cambridge University Press

torture and murder of human rights activists and journalists, such as Jamal Khashoggi, by selling powerful surveillance technology to authoritarian governments."[54] The Global Magnitsky Act, passed in 2016 in the wake of human rights abuses in Russia, "authorizes the President to impose economic sanctions and deny entry into the United States to any foreign person identified as engaging in human rights abuse or corruption."[55] Led by Senator Ron Wyden (D-OR) and House Intelligence Committee Chairman Rep. Adam Schiff (D-CA), the lawmakers have called for sanctions against four companies in particular—NSO Group, "the United Arab Emirates cybersecurity company DarkMatter, and European online bulk surveillance companies Nexa Technologies and Trovicor."[56] DarkMatter drew attention in September 2021 when three former members of the U.S. military and intelligence community entered into a deferred prosecution agreement with the Justice Department for their alleged violations of U.S. export controls and computer crime laws during their time working for the company.[57]

NSO Group's future is uncertain, but it was not the first and will not be the last spyware firm.[58] After the Commerce Department placed NSO on the Entity List, the company's incoming CEO resigned, citing the "'special circumstances that [had] arisen.'"[59] In addition, the European parliament announced in February 2022 that it would "launch a committee of inquiry into the Pegasus spyware scandal."[60] As a result of these investigations and adverse actions, NSO is "in danger of defaulting on its debts" and "exploring options," which include refinancing or selling the firm entirely.[61] Two U.S. funds that are potential buyers have also discussed shutting down Pegasus production.[62] However, even if NSO exits the spyware business, other firms will enter the market.[63]

[54] House Comm. on Oversight & Reform Press Release, Maloney, Wyden, Schiff and Meeks Lead House and Senate Democrats in Calling for Magnitsky Act Sanctions Against Companies That Enable Human Rights Abuses (Dec. 15, 2021), *at* https://oversight.house.gov/news/press-releases/maloney-wyden-schiff-and-meeks-lead-house-and-senate-democrats-in-calling-for [https://perma.cc/SX94-R33T].

[55] Cong. Res. Serv., The Global Magnitsky Human Rights Accountability Act (2020), *at* https://crsreports.congress.gov/product/pdf/IF/IF10576; *see also* Global Magnitsky Human Rights Accountability Act, Pub. L. No. 114-328 (2016).

[56] Joseph Menn & Joel Schectman, *U.S. Lawmakers Call for Sanctions Against Israel's NSO, Other Spyware Firms*, Reuters (Dec. 15, 2021), *at* https://www.reuters.com/world/us/exclusive-us-lawmakers-call-sanctions-against-israels-nso-other-spyware-firms-2021-12-15.

[57] Dep't of Justice Press Release, Three Former U.S. Intelligence Community and Military Personnel Agree to Pay More Than $1.68 Million To Resolve Criminal Charges Arising from Their Provision of Hacking-Related Services to a Foreign Government (Sept. 14, 2021), *at* https://www.justice.gov/opa/pr/three-former-us-intelligence-community-and-military-personnel-agree-pay-more-168-million [https://perma.cc/7NRF-JW66].

[58] Nakashima, *supra* note 45 (noting earlier spyware firms, such as Hacking Team and Gamma).

[59] Steven Scheer & Dan Williams, *CEO-Designate of NSO Spyware Firm Quits Following U.S. Blacklist*, Reuters (Nov. 11, 2021), *at* https://www.reuters.com/technology/new-ceo-nso-spyware-firm-quits-citing-us-blacklist-israeli-media-say-2021-11-11.

[60] Boffey, *supra* note 13.

[61] Yaacov Benmeleh & Eliza Ronalds-Hannon, *Spyware Firm NSO Mulls Shutdown of Pegasus, Sale of Company*, Bloomberg (Dec. 13, 2021), *at* https://www.bloomberg.com/news/articles/2021-12-13/spyware-firm-nso-mulls-shutdown-of-pegasus-unit-sale-of-company.

[62] *Id.*

[63] Christopher Bing & Raphael Satter, *iPhone Flaw Exploited by Second Israeli Spy Firm – Sources*, Reuters (Feb. 3, 2022), *at* https://www.reuters.com/technology/exclusive-iphone-flaw-exploited-by-second-israeli-spy-firm-sources-2022-02-03.

https://doi.org/10.1017/ajil.2022.13 Published online by Cambridge University Press