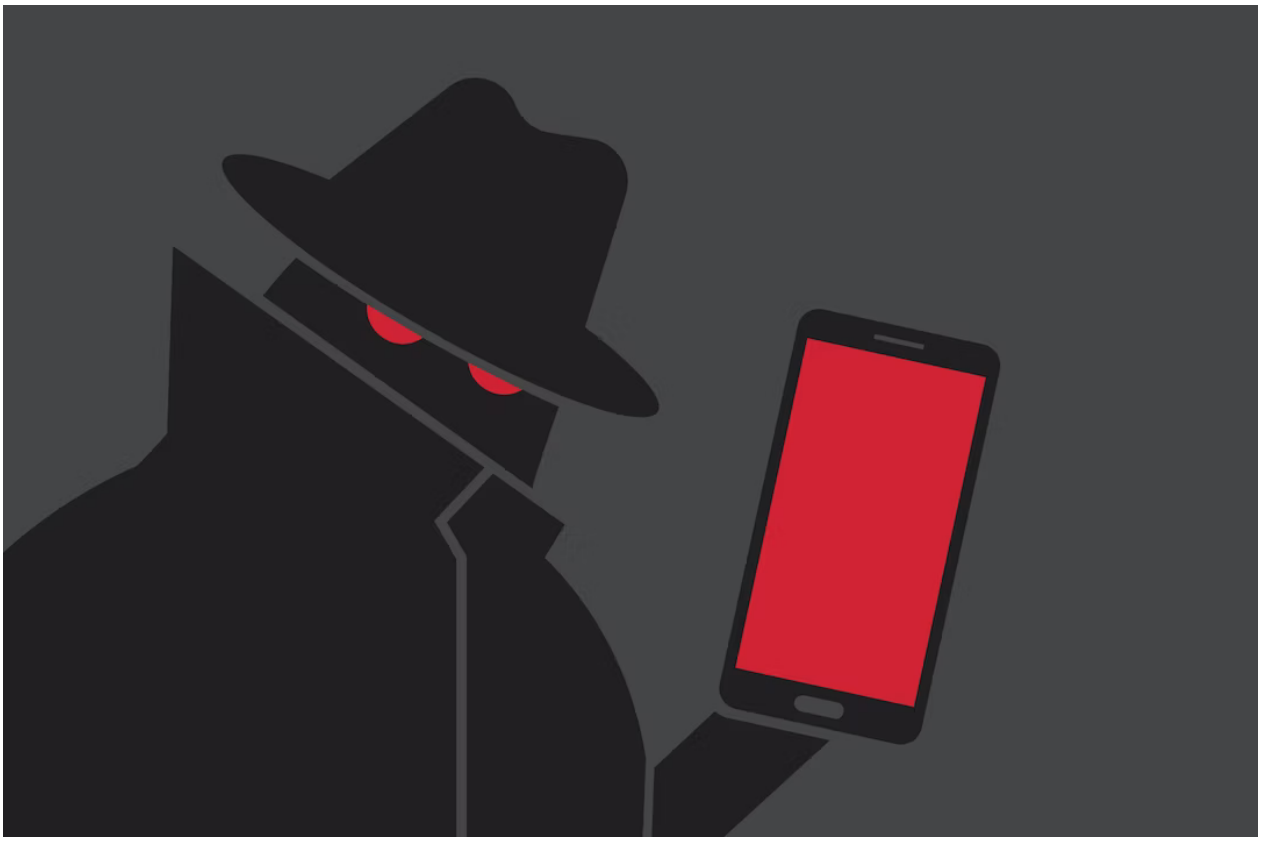
THIRD WAY

MEMO *Published June 22, 2023 • 15 minute read*

Unregulated Spyware's Threat to National Security



Mike Sexton
Senior Policy Advisor for Cyber and Artificial Intelligence
@MikeESexton

Commercial spyware is a dual-use technology: it can theoretically be an essential last-resort tool for the most critical national security and law enforcement investigations, but it carries profound risk of abuse. Criticisms of spyware proliferation have focused primarily on its human rights violations, such as its abusive deployment against journalists, activists, and others merely exercising their freedom of expression and assembly. But like every dual-use technology – drones, small arms, nuclear materials, or biological agents – the proliferation of spyware poses a national security threat to the United States and its allies and partners unless the international community develops and enforces firm regulations and export controls governing their development and sale.

In the past, if a government sought to acquire the capabilities of modern commercial spyware, it would have to cultivate the requisite talent base, recruit scores if not hundreds of government hackers from this community, and maintain that workforce indefinitely. [1] Today, that workforce can be centralized in a single company headquartered abroad, exporting to dozens of client

governments with little regard for how the tools sold are used. The result is as if the Manhattan Project were undertaken by a corporate R&D department in a faraway land and the spread of nuclear weapons was driven not by generals and spy chiefs, but shareholders and c-suites.

This status quo is dangerous and unsustainable. When cybersecurity researchers discover a vulnerability in a widely used device or application, they have a financial incentive – and, many would argue, a moral duty – to report that vulnerability to the developer – a process known as a "bug bounty." However, the emergence of the commercial spyware industry creates a perverse incentive for researchers to sell or use their discovery to help develop hacking tools instead, which not only harms the targets of these hacking tools, but systemically puts all users of the underlying vulnerable technology at risk.

This paper lays out known instances when the spyware industry has presented a direct criminal, counterintelligence, and national security threat to the United States, supported by forensic evidence, press reporting, and even testimony of mercenary hackers turned FBI informants. If spyware is a necessary evil to protect national security interests, more work needs to be done to rein in unacceptable behavior and rebalance the incentives and equities involved.

Takeaways

- Spyware companies' defense against human rights violations is that they are essential partners for intelligence and law enforcement. In many cases, the opposite is true: they have been profound counterintelligence and criminal threats.
- The most notorious developer of spyware, NSO Group, is a defendant in three US lawsuits alleging criminal violations of the Computer Fraud and Abuse Act by Meta, Apple, and journalists at the Salvadoran newspaper El Faro.
- The White House has determined that commercial spyware has infected at least 50 US government employees – a clear counterintelligence threat risking compromise of classified information. This is undoubtedly the tip of the iceberg.
- Government operators of spyware have impersonated US government officials and conducted criminal hacking against US citizens and government employees, as well as lawful US residents on American soil. These are all federal crimes.

Spyware Striking the United States

Below is a noncomprehensive list of known cases of foreign commercial spyware being deployed on American soil, on American citizens, and on American government officials. This list features cases of spyware breaches where the program has been developed by private companies and launched under the aegis of a foreign government. It excludes hacking incidents that could be attributed to tools developed internally by a foreign government agency, or tools deployed by a private party without government involvement – these are outside the scope of this report.

The lack of transparency or centralized reporting makes it likely that there have been more commercial spyware operations detrimental to American national security than we know of. Spyware companies like NSO Group claim not to keep tabs on whom their customers target using their products; [2] while that assertion may strain credulity, we can at least infer they do not do for the purposes of firing abusive customers, which has historically only resulted from outside revelations and contingent political pressure. Spyware customers – foreign governments – are effectively left to hold themselves accountable, which in practice means little to nothing.

Surveilling Michelle Obama

In 2015, First Lady Michelle Obama's staff were organizing the itinerary for a stop in Qatar as part of a weeklong trip to the Middle East. [3] Her time in Qatar would include a visit to Al Udeid Air Base, home to 10,000 American troops, and a speech at a summit organized by the Qatar Foundation and its chair, Sheikha Moza bint Nasser – the mother of the country's ruling Emir.

Unbeknownst to the First Lady, her extensive coordination with Sheikha Moza was swept up by a company called CyberPoint, which had hacked and been surveilling the royal consort at the behest of the Gulf state's nearby rival, the United Arab Emirates. More shocking still: CyberPoint was an American company, staffed predominantly with former NSA hackers, ostensibly contracting with the permission of the US State Department. Surveilling the First Lady – if only incidentally – sufficed to convince at least one ex-NSA analyst on the team that his mission had strayed so far from preserving national security as to be unrecognizable.

Surveilling the First Lady – if only incidentally – sufficed to convince at least one ex-NSA analyst on the team that his mission had strayed so far from preserving national security as to be unrecognizable.

The most outrageous details of the case have also made it easiest to remedy. CyberPoint's contract with the UAE led to an FBI investigation that culminated in the deferred prosecution of three

American contractors. [4] Congress went on to ban American spies from working as mercenaries for foreign governments for 30 months after leaving civil service [5] – a significant first step to stemming the tide of proliferation. While CyberPoint still exists, it is no longer reported to take on offensive operation contracts; its contract with the Emirati government was supplanted by the native Emirati firm DarkMatter.

Jamal Khashoggi, The Washington Post, and Jeff Bezos

When Washington Post columnist and Virginia resident Jamal Khashoggi was murdered, media reporting broadly framed the event as the assassination of a Saudi journalist/critic at the hands of his own government. The American public understood it as an appalling human rights violation, but with little clear or direct link to the United States or its interests. [6]

But Khashoggi's surveillance and assassination absolutely ran roughshod over American institutions and interests, and spyware played an integral role in the killing – more than many observers realize. [7] Jeff Bezos, who bought the Washington Post in 2013, [8] was also allegedly hacked with spyware sent directly by Saudi Crown Prince Mohammed bin Salman (also known as MBS) five months before Khashoggi's killing. [9]

Bezos and the Crown Prince had been casually conversing via WhatsApp before MBS, unsolicited, sent an unusually large video file, [10] after which the data egressing Bezos's phone skyrocketed by 29,000%. The data egress – circumstantial evidence of exfiltration by some hacker – combined with further advanced forensic analysis led investigators to conclude with high confidence that MBS's suspicious video attachment was, in fact, infected with malware that caused the security breach.

Bezos and the Crown Prince had been casually conversing via WhatsApp before MBS, unsolicited, sent an unusually large video file, after which the data egressing Bezos's phone skyrocketed by 29,000%.

Bezos and his seasoned security consultant, Gavin De Becker, concluded that the hacking of his phone was linked to a story in the National Enquirer revealing that Bezos had been having an affair with television anchor Lauren Sanchez. [11] The story, published eight months after Bezos's phone was allegedly infected (and three months after Khashoggi was killed), featured private text messages between Bezos and Sanchez. [12]

Although the National Enquirer publicly and vehemently claimed that its source was instead Sanchez's brother, the Wall Street Journal reported that the tabloid was *already* investigating the affair when it contacted him. [13] Coinciding with the circumstantial evidence of the hack is the National Enquirer's indecorously cozy relationships with President Donald Trump [14] and MBS [15] – both with longstanding and well-documented grudges against the Washington Post and, by extension, Bezos.

Bezos was not hacked because he is rich; he was hacked because he owns one of the most influential newspapers in America. A foreign autocrat hacking and blackmailing an American newspaper owner for the paper's critical coverage of his regime is a brazen assault on the national security interests of the United States, as well as its institutions and principles.

Ben Hubbard and the New York Times

Ben Hubbard, then the Beirut bureau chief at the New York Times, was also targeted with Pegasus by the Saudi government. [16]

Hubbard, a US citizen, [17] was targeted twice in 2018 with malicious links sent via text and WhatsApp but avoided infection by not clicking on them. [18] In 2020 and 2021, Hubbard was probed again – this time, with more powerful and insidious "zero-click" spyware, infecting his phone without him clicking any link or taking any direct action.

In 2020 and 2021, Hubbard was probed again – this time, with more powerful and insidious "zero-click" spyware, infecting his phone without him clicking any link or taking any direct action.

Hubbard's hacking gives lie to NSO Group's claim that Pegasus cannot be wielded against "US targets." [19] Pegasus may be unable to target US +1 country code phone numbers, but it lacks the digital code or human oversight to prevent it from being deployed against American citizens with foreign phone numbers like Hubbard, who was residing in Lebanon.

> Under international standards, all phone numbers globally begin with a country code, often omitted for domestic calls/texts. The US code is +1, as in +1-202-384-1700. Phone numbers with this prefix code are reportedly immune from Pegasus infection. However, if an American uses a foreign phone number with a non-US country code like Lebanon (+961), or if someone with such a number travels to the US, they have no such protection.

Hubbard was abroad, using a non-US phone number, and working as a journalist when he was hacked with Israeli technology by a Saudi operator. This shows that our national security protection against spyware is only as solid as foreign players allow it to be: in practice, not solid at all.

Spyware Infecting US Personnel in Africa

The impacts of spyware proliferation have been felt around the world, including in sub-Saharan Africa. Here, as in the UAE, the United States has enabled the problem, with the CIA paying for Djibouti to acquire Pegasus the same year Jamal Khashoggi was murdered. [20] This deal was brokered despite fact that the Horn of Africa country of about one million is ruled by a hereditary dictatorship with a well-documented history of human rights abuses, [21] including arbitrary detention and torture of government critics.

The proliferation of Pegasus in Africa has also spread 1000 miles southwest to Uganda, an authoritarian state. [22] In Uganda, Pegasus has boomeranged to infect 11 iPhones belonging to officials at the US Embassy in Kampala using non-US phone numbers, like Ben Hubbard's. [23]

Next door in Rwanda, the government has used or considered using Pegasus to target over 3,500 journalists, politicians, and members of civil society, according to the Pegasus Project. [24] Victims of Rwanda's Pegasus operations include Carine Kanimba, the American [25] daughter of Paul Rusesabagina, the Rwandan hotel manager who sheltered over a thousand refugees during the 1994 Rwandan genocide.

In total, the White House has determined that at least 50 US government employees in ten countries have been infected by commercial spyware. [26] Unlike civilian victims of spyware, US government employees cannot bring their devices to forensic investigators like Amnesty Tech or Citizen Lab because their devices contain government-classified information, meaning the total number of US government devices infected could well be even higher. But even the conservative estimate of 50 government victims should suffice to prompt the US to take its foot off the gas spreading spyware, like in Djibouti, if not resolutely slam the brakes.

El Salvador and El Faro

El Salvador illustrates the paradox of spyware and the need for better regulation and protection. Ravaged for decades by gang violence, few countries arguably have a greater need to equip law enforcement with cutting edge technology like spyware. However, while it is likely spyware has been justifiably deployed to combat gangs like MS-13, it has still inexcusably ensnared innocent Salvadorans and even Americans.

Since 2019, El Salvador has been ruled by President Nayib Bukele, who has called himself "the coolest dictator in the world." [27] He has made El Salvador the first country to establish Bitcoin as

legal tender and spearheaded a crackdown that has arrested over 65,000 suspected gang members – often without charge. [28] The most evocative recurring images of his presidency are of Bitcoin ATMs lining the streets and suspected gangsters herded half-naked on prison floors like livestock. [29]

He is popular and feared. Bukele's bare-knuckled approach to murderous gangs like MS-13 have netted him approval ratings over 75% and as high as 91% [30] – the highest in Latin America. He betrays no reticence as foreign leaders raise the alarm over his human rights abuses and assaults on the country's courts and legislature. Instead, he contrasts this criticism with his soaring approval ratings and revered status in the global crypto community to fashion himself as an iconoclast and visionary, carrying El Salvador from corruption and anarchy to futuristic prosperity.

Although Bukele relishes the limelight, his relationships with journalists quickly sour once they become adversarial. One dauntless Salvadoran online newspaper that has especially piqued Bukele's ire is El Faro. After publishing one critical story of Bukele's gang policies, the president announced an investigation into El Faro for money laundering.

Bukele employed Pegasus in his campaign to surveil and intimidate El Faro, including a 26-year-old journalist from Indiana named Roman Gressier. [31] was hacked shortly after publishing an article about the US State Department labeling a senior Bukele cabinet minister as corrupt. He was then hacked three more times over the span of about a month.

Gressier is a dual US and French citizen who became fluent in Spanish as a young Mormon missionary to Hispanic immigrants in Washington state. Before even knowing he was hacked, Gressier was sensitive to the threat of spyware and possible blackmail – he was openly bisexual to close friends and coworkers, but he avoided making this public due to anti-LGBTQ stigma in El Salvador.

After a pair of Salvadoran journalists at El Faro and GatoEncerrado discovered their strangely malfunctioning smartphones had, in fact, been hacked with Pegasus, El Faro held an emergency meeting. The newspaper agreed to have all employees' devices forensically analyzed – ultimately discovering almost the entire organization had been infected. The journalists' sources felt their trust had been betrayed, and many of the hacking victims have since fled the country.

The story of Gressier's hacking is sadly familiar, but how he has responded to it is historic. In November 2022, Roman Gressier, 15 of his El Faro colleagues, and the Knight First Amendment Institute filed a lawsuit against NSO Group in US federal court for violating the 1986 Computer Fraud and Abuse Act [32] – the first time an American victim of Pegasus has sued NSO Group in US court. [33] The legal case adds to the crescendo of pressure to hold NSO Group and its investors accountable for the company's malfeasance.

Hacking a Journalist's Son

Mexico has been a prodigious user of spyware. To NSO Group, Mexico has been a Pegasus success story – although the company categorically refuses to name its client governments, it has claimed its spyware was instrumental in the 2016 capture of the infamous Mexican drug lord El Chapo. [34]

But Mexico has used Pegasus to track more than just drug cartels. Carmen Aristegui, an indefatigable journalist, also drew the disdain of the Mexican government for her critical coverage of Enrique Peña Nieto, Mexico's president from 2012 to 2018. Her website, Aristegui Noticias, reported in 2014 that Peña Nieto's wife purchased a home from a contractor close to the president worth $7 million – far outside her family's budget.

Aristegui's report of the real estate deal was impactful – the first lady was forced to give up the home, which became popularly known as the Casa Blanca, and the president issued a public apology. But in the aftermath, Aristegui's office was burglarized, she faced multiple lawsuits, and the Mexican government used Pegasus not only to hack and surveil Aristegui, but her 16-year-old son Emilio – while he was on American soil. [35]

Even as norms against using spyware against civilians have eroded, using it to hack a child remains viscerally shocking. "What did they want to know about my son, Emilio? Why did the government… want to know about the friendships, the communication my son had, his photos, what he does, what he says in real time?" Carmen said. Perhaps Carmen, as a journalist, may have spoken to someone of interest to Mexican law enforcement, like a member of a drug cartel. Hacking her teenage son, however, serves no apparent purpose but to heighten surveillance on Carmen herself – to effectively treat her journalism as criminal activity.

According to Citizen Lab, Emilio received at least 21 messages with links to infect his phone with Pegasus. [36] The texts used a variety of methods to manipulate Emilio into clicking the infected links, including impersonating the US Embassy in Mexico. It is worth noting that while he may not have been using an American phone number, Emilio was residing in Massachusetts while he was being targeted. Besides being morally repugnant, the hacking of Emilio on American soil violates the US Computer Fraud and Abuse Act; impersonating the US Embassy to do so is also a crime. [37]

Spyware Proliferation: The Paradox

Is spyware worth the cost? Spyware companies like NSO Group are steadfast that their products are crucial tools for government agencies around the world to investigate serious crime and prevent terrorism. The capture of El Chapo shows that it can be a powerful tool to go after violent and lawless organizations. But it can just as easily go after the innocent as well. Journalists, civil society, and some government bodies have chronicled spyware industry abuses ranging for human rights violations to criminal activity and even threats against national security for the United States and NATO. The unregulated spyware industry is in desperate need of regulation.

TOPICS

ENDNOTES

1. Because spyware and other hacking tools rely on software vulnerabilities that are continuously discovered and patched by their respective developers, hacking capabilities steadily and ineluctably "rust" – a spyware payload that successfully hacked a smartphone in 2020 is unlikely to work on the same device in 2023 after it has undergone numerous software updates. Thus a sizeable and stable workforce is needed to retain any kind of offensive cyber capabilities – discovering new vulnerabilities and developing exploits as the software landscape shifts.

2. Kirchgaessnner, Stephanie. "How NSO Became the Company Whose Software Can Spy on the World." The Guardian, 23 July 2021, www.theguardian.com/news/2021/jul/23/how-nso-became-the-company-whose-software-can-spy-on-the-world. Accessed 25 May, 2023.

3. Perlroth, Nicole. "Chapter 11." *This Is How They Tell Me the World Ends: The Cyberweapons Arms Race*, Bloomsbury Publishing, 2023, pp. 161–162.

4. Zetter, Kim. "Former NSA Hacker Describes Being Recruited for UAE Spy Program." *Zero Day*, 20 Sept. 2021, https://zetter.substack.com/p/former-nsa-hacker-describes-being. Accessed 23 March, 2023.

5. Bing, Christopher, and Joel Schectman. "U.S. Bars Ex-Spies from Becoming 'Mercenaries,' Following Reuters Series." *Reuters*, Thomson Reuters, 16 Mar. 2022, https://www.reuters.com/world/us/us-bars-ex-spies-becoming-mercenaries-following-reuters-series-2022-03-16/. Accessed 23 March, 2023.

6. In this New York Times article, published while details of the killing were still slowly coming to light, there is no mention that Khashoggi was affiliated with the Washington Post and his residency in Virginia is only noted in a photo caption: Specia, Megan. "Jamal Khashoggi's Killing: Here's What We Know" *The New York Times*, 19 Oct. 2018, www.nytimes.com/2018/10/19/world/middleeast/jamal-khashoggi-case-facts.html. Accessed 29 March, 2023.

7. Public reporting has not revealed the provenance of the spyware that infected Bezos's phone. Bezos was presumably using a US, 1 country code phone number, and NSO's assertion that Pegasus cannot infect such phones has not been disproven. It is possible, if not likely, that Saudi Arabia procured the spyware from another source, such as the government-run DarkMatter in the neighboring ally, the UAE.

8. Farhi, Paul. "Washington Post to Be Sold to Jeff Bezos, the Founder of Amazon." The Washington Post, WP Company, 5 Aug. 2013, https://www.washingtonpost.com/national/washington-post-to-be-sold-to-jeff-bezos/2013/08/05/ca537c9e-fe0c-11e2-9711-3708310f6f4d_story.html. Accessed 3 April, 2023.

9. Kirchgaessner, Stephanie. "Jeff Bezos Hack: Amazon Boss's Phone 'Hacked by Saudi Crown Prince'." The Guardian, Guardian News and Media, 22 Jan. 2020, https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince. Accessed 3 April, 2023.

10. Zetter, Kim, and Joseph Cox. "Here Is the Technical Report Suggesting Saudi Arabia's Prince Hacked Jeff Bezos' Phone." VICE, 22 Jan. 2020, https://www.vice.com/en/article/v74v34/saudi-arabia-hacked-jeff-bezos-phone-technical-report. Accessed 3 April, 2023.

11. De Becker, Gavin. "Bezos Investigation Finds the Saudis Obtained His Private Data." The Daily Beast, The Daily Beast Company, 31 Mar. 2019, https://www.thedailybeast.com/jeff-bezos-investigation-finds-the-saudis-obtained-his-private-information?ref=scroll. Accessed 3 April, 2023.

12. Robertson, James, et al. "Jeff Bezos' Raunchy Text Messages That Prove Illicit Affair." National Enquirer, 21 Jan. 2019, https://www.nationalenquirer.com/videos/jeff-bezos-lauren-sanchez-text-messages-affair-scandal/. Accessed 7 April, 2023.

13. Rothfeld, Michael, et al. "How the National Enquirer Got Bezos' Texts: It Paid $200,000 to His Lover's Brother." The Wall Street Journal, Dow Jones & Company, 19 Mar. 2019, https://www.wsj.com/articles/how-the-national-enquirer-got-bezos-texts-it-paid-200-000-to-his-lovers-brother-11552953981. Accessed 3 April, 2023.

14. Rutenberg, Jim. "More Powerful than a Russian Troll Army: The National Enquirer." The New York Times, The New York Times, 16 Dec. 2018, https://www.nytimes.com/2018/12/16/business/media/national-enquirer-trump-mistresses.html. Accessed 3 April, 2023.

15. West, James. "National Enquirer Investigated by FBI over Possible Saudi Influence Peddling." Mother Jones, 15 Aug. 2019, https://www.motherjones.com/politics/2019/08/national-enquirer-ami-fbi-bezos-saudi-arabia-investigation/. Accessed 3 April, 2023.

16. Marczak, Bill, et al. "Stopping the Press: New York Times Journalist Targeted by Saudi-Linked Pegasus Spyware Operator." The Citizen Lab, 28 Jan. 2020, https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/. Accessed 3 April, 2023.

17. Ben Hubbard was born and raised in Colorado. "Ben Hubbard." The New York Times, The New York Times, https://www.nytimes.com/by/ben-hubbard. Accessed 4 April, 2023.

18. Hubbard, Ben. "I Was Hacked. the Spyware Used against Me Makes Us All Vulnerable." The New York Times, The New York Times, 24 Oct. 2021, https://www.nytimes.com/2021/10/24/insider/hacking-nso-surveillance.html. Accessed 4 April, 2023.

19. Vavra, Shannon. "Spyware Firm's Claims That It Can't Target Americans Don't Add Up." The Daily Beast, The Daily Beast Company, 19 July 2021, https://www.thedailybeast.com/nso-group-spyware-firms-claims-that-it-cant-target-americans-dont-add-up. Accessed 4 April, 2023.

20. Bergman, Ronen, and Mark Mazzetti. "The Battle for the World's Most Powerful Cyberweapon." The New York Times, The New York Times, 28 Jan. 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html. Accessed 6 April, 2023.

21. Norman, Joshua. "The World's Enduring Dictators: Ismael Omar Guelleh, Djibouti." CBS News, CBS Interactive, 11 June 2011, https://www.cbsnews.com/news/the-worlds-enduring-dictators-ismael-omar-guelleh-djibouti/. Accessed 6 April, 2023.

22. Atuhaire, Patience. "Uganda Anti-Homosexuality Bill: Life in Prison for Saying You're Gay." BBC News, BBC, 22 Mar. 2023, https://www.bbc.com/news/world-africa-65034343. Accessed 6 April, 2023.

23. Srivastava, Mehul. "The Secret Uganda Deal That Has Brought Nso to the Brink of Collapse." Ars Technica, 21 Dec. 2021, https://arstechnica.com/information-technology/2021/12/the-secret-uganda-deal-that-has-brought-nso-to-the-brink-of-collapse/. Accessed 6 April, 2023.

24. "Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware." Amnesty International, 19 July 2021, https://www.amnesty.org/en/latest/press-release/2021/07/rwandan-authorities-chose-thousands-of-activists-journalists-and-politicians-to-target-with-nso-spyware/. Accessed 6 April, 2023.

25. Kirchgaessner, Stephanie. "Hotel Rwanda Activist's Daughter Placed under Pegasus Surveillance." The Guardian, Guardian News and Media, 19 July 2021, https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance. Accessed 6 April, 2023.

26. "Background Press Call on the President's Executive Order on Commercial Spyware." The White House, The United States Government, 27 Mar. 2023, https://www.whitehouse.gov/briefing-room/press-briefings/2023/03/27/background-press-call-on-the-presidents-executive-order-on-commercial-spyware/. Accessed 6 April, 2023.

27. Youkee, Mat. "Nayib Bukele Calls Himself the 'World's Coolest Dictator' – but Is He Joking?" The Guardian, Guardian News and Media, 26 Sept. 2021, https://www.theguardian.com/world/2021/sep/26/naybib-bukele-el-salvador-president-coolest-dictator. Accessed 4 April, 2023.

28. "El Salvador's Congress Extends Anti-Gang Crackdown." AP NEWS, Associated Press, 17 Mar. 2023, https://apnews.com/article/el-salvador-gangs-crackdown-human-rights-8a2cbda6b2204864700 5c5afcca847cf. Accessed 4 April, 2023.

29. Blitzer, Jonathan. "The Rise of Nayib Bukele, El Salvador's Authoritarian President." The New Yorker, 5 Sept. 2022, https://www.newyorker.com/magazine/2022/09/12/the-rise-of-nayib-bukele-el-salvadors-authoritarian-president. Accessed 5 April, 2023.

30. Galdamez, Eddie. "Despite Claims of Authoritarianism, President Bukele's Popularity Continues to Be Strong in El Salvador." Global Voices, 22 Feb. 2021, https://globalvoices.org/2021/02/22/despite-claims-of-authoritarianism-president-bukeles-popularity-continues-to-be-strong-in-el-salvador/. Accessed 4 April, 2023.

31. Farrow, Ronan. "A Hacked Newsroom Brings a Spyware Maker to U.S. Court." The New Yorker, 30 Nov. 2022, https://www.newyorker.com/news/news-desk/a-hacked-newsroom-brings-a-spyware-maker-to-us-court-pegasus. Accessed 5 April, 2023.

32. "El Faro Journalists, Knight Institute Sue Nso Group over Spyware." Knight First Amendment Institute, Columbia University, 30 Nov. 2022, https://knightcolumbia.org/content/el-faro-journalists-knight-institute-sue-nso-group-over-spyware. Accessed 5 April, 2023.

33. WhatsApp and Apple – platforms exploited by NSO Group – have also sued NSO in US court in 2019 and 2021 respectively. Other victims of Pegasus have sued NSO and the spyware-operating governments of Saudi Arabia and the UAE in UK court.

34. Bergman, Ronen. "Exclusive: How Mexican Drug Baron El Chapo Was Brought down by Technology Made in Israel." Ynetnews, Ynetnews, 10 Jan. 2019, https://www.ynetnews.com/articles/0,7340,L-5444330,00.html. Accessed 6 April, 2023.

35. Devereaux, Ryan, and Thiago Dezan. "Mexican Journalist Carmen Aristegui Slams Government Spyware Targeting Her Teenage Son." The Intercept, The Intercept, 18 July 2017, https://theintercept.com/2017/07/18/mexican-journalist-carmen-aristegui-slams-government-spyware-targeting-her-teenage-son/. Accessed 6 April, 2023.

36. Scott-Railton, John, et al. "Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware." The Citizen Lab, 19 June 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/. Accessed 6 April, 2023.

37. 25 CFR § 11.432.