Winter 2-1-2024

Pegasus in Hungary: Analyzing Hungary's Use of Pegasus on journalists with Lessig's Four Modalities of Regulation

Katherine Kuhl

Pegasus Spyware in Hungary:

Analyzing Hungary's use of Pegasus on journalists with Lessig's Four Modalities of Regulation

Katherine Kuhl
B.A. International Studies, Global Track
Fordham University

Thesis Advisor: William Akoto, Ph.D.
Secondary Advisor: Katherine Wilson, Ph.D.

Dec 23, 2023

Table of Contents

Abstract:

Over the last decade, technological advancements in the realm of cybersecurity has led to the growth of a multi-billion dollar commercial spyware industry, which puts highly privacy-invasive surveillance tools in the hands of both autocratic and democratic nations. This paper seeks to better understand why, and how democratic countries have been able to access these tools, and why they are willing to risk the reputational costs associated with illegal use of spyware. A field of scholarship is developing which seeks to find possible ways of eliminating or reducing the misuse of spyware on an international scale, under the presumption that finding ways to diminish the capacity of spyware firms to sell their products to governments who have a track of human rights abuse will translate into a meaningful reduction of privacy crimes aided by spyware. However, focused examination on the underlying factors or forces that presumably motivate, or incentivize a 'democratic' country to use spyware in the first place, and why other 'democratic' countries do not take a stronger stance against such misuse, is lacking. This paper will try to conduct such an analysis in a case study focusing on Hungary's use of Pegasus spyware to surveil four journalists. The analysis will use Lessig's "four modalities of regulation" – laws, markets, norms, and architecture (as expounded in his book Code 2.0 (2006)) as an analytical framework, to conceptually organize and understand the forces that hindered or motivated Hungary's decision to use Pegasus on journalists, and how Hungary's case may provide insight into the viability of proposals for future regulations.

Introduction

Journalists around the world are repressed by various means. Surveillance is one of them. Over the course of the last decade, government use of commercial spyware has increased significantly, with some of that uptick going towards the illegal surveillance of journalists, dissidents, government officials, and even heads of state. Pegasus is the most powerful and sophisticated spyware on the market; at least 180 journalists were listed as potential Pegasus targets – four of the confirmed are Hungarians.[1] In the spring of 2022, the European Parliament put together the PEGA committee to investigate the state of the spyware industry and spyware misuse in the EU.[2] The committee found widespread abuse – not only in Hungary – but in Greece, Spain, and Poland as well.[3] But why did the EU need the PEGA committee in the first place? What makes spyware so susceptible to misuse, and why have seemingly democratic countries been using it, and in some cases, exporting it? Scholarship on spyware regulation addresses these questions, primarily with a focus on combating the misdeeds of the spyware *industry*, with state misuse as the secondary issue. Their consensus is that the best plan of attack is *to regulate producers*: to set constraints on firms into becoming human rights abiding entities, followed by blocking states with 'bad track records' from partaking in what 'properly'-regulated firms have to offer. But what about the consumers, the governments who purchase and use spyware? Other democratic states haven't used – or have not been publicly caught using –

[1]"Massive data leak reveals Israeli NSO spyware used to target activists, journalists, and political leaders globally", Amnesty International, July 19, 2021, https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.
[2] Spencer Levitt, "The European Parliament's PEGA Committee: A Regional Effort to Constrain Spyware Technology", UCI Law International Justice Clinic, January 25, 2023, https://ijclinic.law.uci.edu/2023/01/25/the-european-parliaments-pega-committee-a-regional-effort-to-constrain-spyware-technology/.
[3] E.U. European Parliament , *Investigation of the use of Pegasus and equivalent spyware (Recommendation),* June 15, 2023, 6, https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf.

spyware for illegal surveillance purposes. Why have these governments not taken greater initiative towards curtailing the spread and use of commercial spyware within government?

Hungary offers a prime case study for these questions because of its use of Pegasus to repress journalists, and because it is an increasingly authoritarian state, despite its membership in the European Union. Lessig's Four Modalities of Regulation will be used to analyze the ways in which the state overcame current regulatory constraints in order to use Pegasus, as well as the features that make spyware an enduring tool for illegal surveillance. These findings will be used to evaluate the strength of current regulatory proposals, based on how democratic states have responded to cases like Hungary, and the unique challenges posed by trying to regulate the use of commercial spyware in state surveillance operations.

Background

Hungary's illegal surveillance of journalists is made possible by the strength of the spyware industry (estimated annual sales of $12 billion)[4], an Israeli technology company, and the most powerful spyware tool on the market, Pegasus.

What is spyware?

Spyware is a type of software used to perform certain behaviors on an electronic device without obtaining the permission of the device's owner to do so. Different kinds of spyware vary in their level of sophistication in two distinct ways: the means by which they infect a device, and their ability to gather or harvest information from the device[5]. An example of a common, less sophisticated type of spyware infection would be when a user clicks a link on a pop-up window,

[4] Steven Feldstein and Brian Kot, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses" Carnegie Endowment for International Peace, March 2023, 6, https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf.
[5] Gretchen Nobahar, "Spyware" in *Privacy Rights in the Digital Age,* edited by Jane E. Kirtley and Michael Shally-Jensen. Grey House Publishing, 2019, accessed September 25, 2023, https://search.credoreference.com/articles/Qm9va0FydGljbGU6NDc5NTYyNg==.

or opens an email attachment from an unknown source, and their computer shuts down or restarts. Such a disruption to the computer's functioning might signal to the owner that their computer is newly infected by some kind of malware. Some forms of spyware perform just a single function, like tracking device location or the keystrokes on a computer. At the top of the spyware ladder is Pegasus, which has the ability to unlock and transmit the entire contents of a mobile device, in addition to taking control of the device's microphone and camera – no user input necessary.

What is Pegasus?

Shalev Hulio, Niv Karmi, and Omri Lavie established NSO Group, a surveillance technology firm based in Israel in 2010, and started marketing Pegasus to clients the following year.[6] Pegasus is a spyware, and is able to gain access to a mobile device's operating system remotely. It is considered a zero-click spyware, because it is able to infect devices without any input from the device's owner. The engineers behind Pegasus utilize zero-day vulnerabilities, which are bugs in software or hardware that have either not been 'patched', or discovered by those who own and manage the software. An entire industry is based off of hackers finding and selling zero-day vulnerabilities – companies like Apple and Google pay up to 1 million dollars in exchange for zero-day vulnerabilities found in their software[7]. NSO Group helps their clients infect target phones by utilizing sophisticated combinations of zero-day vulnerabilities found in the operating systems of devices as well as apps available to those devices.

NSO's success frustrates the makers of exploited software, whose reputation and profitability depends in part on being able to assure consumers that their data will be secure. In 2019, WhatsApp filed a lawsuit against NSO Group in the state of California. In their initial

[6] Sean D. Kaster and Prescott C. Ensign, "Privatized espionage: NSO Group Technologies and its Pegasus spyware", Thunderbird International Business Review, December 1, 2022. **https://doi.org/10.1002/tie.22321**
[7] "Apple Security Bounty Categories", https://security.apple.com/bounty/categories/, accessed December 1, 2023.

filing WhatsApp claimed that the spyware firm had illegally surveilled users of the messaging service by making calls that infect targeted devices. The code received by the target was reengineered such that Pegasus software downloaded to the phone as soon as the device had received the call, regardless of whether the call had been 'picked up' by the owner or not. Once Pegasus was successfully downloaded to the phone, the 'missed call' was deleted from the target's phone, erasing any possible indication to the user that their device had been hacked or interfered with. WhatsApp conducted an investigation with the help of forensic analysts at Citizen Lab (a leading research group focused on the spread of Pegasus and similar surveillance products, based out of the University of Toronto) and discovered that the mobile devices of 1,400 users from 20 different countries had had their mobile device infected with Pegasus through WhatsApp in this way.[8]

Pegasus is considered the most malicious commercially available spyware. The spyware is hard to detect, requiring expert forensic analysis to determine an infection on a device, and is able to gather more information from a device in use than any other means of remote surveillance.[9] The spyware first gained widespread international attention in 2018, after Citizen Lab discovered past infections on the phone of Jamal Khashoggi's wife, and the devices of some of his friends. Khashoggi was a Saudi journalist who worked for the Washington Post and maintained permanent residency in the United States. He was an outspoken critic of Crown Prince Mohammed Bin Salman, which presumably led to his murder and dismemberment when he visited the Turkish Saudi consulate in 2018. As the details of his death began to emerge in the

[8] Citizen Lab, "NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases", University of Toronto, October 29, 2019, https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.; WhatsApp Inc., and Facebook, Inc., v. NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. (United States District Court Northern District of California May 27, 2020), 2, https://www.documentcloud.org/documents/6532395-WhatsApp-complaint.html.

[9] Steven Feldstein and Brian Kot, *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses*, (Washington DC: Carnegie Endowment for International Peace, March 15, 2023) 10, https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf.

proceeding months, his murder became a rallying point for international criticism of Saudi Arabia's human rights record[10].

In 2021 NSO came back into the spotlight. The Pegasus Project, a consortium of journalists, began publishing reports about a list of 50,000 names, originally received by two of the Project's partners, Forbidden Stories and Amnesty International, from an NSO employee, or someone otherwise associated with NSO's operations (the source has never been revealed).[11] At the end of the consortium's investigation, the reporters concluded that the names were at some point potential Pegasus targets, selected by NSO clients. The Pegasus Projects' findings were affirmed by forensic analysis by Amnesty Security Lab and peer-reviewed by Citizen Lab, Approximately 600 government officials were on the list (The Pegasus Project), including some heads of state.[12] The scandal engulfed the firm in a PR crisis, from which the company has never fully recovered. In 2021, in the midst of the Pegasus fallout, the US decided to blacklist NSO Group, which allegedly put the firm on the verge of bankruptcy. NSO Group has had several different CEOs and owners in the time since, but it has not completely fallen apart as some had hoped it would.

The Spyware Industry

Over the last twenty years, the commercial spyware industry has been perfecting the technology that it sells to government agencies and officials. The industry-wide position is that their products are only used to combat serious crime like terrorism and pedophilia. Spyware firms rarely put themselves in the public eye, aside from periodic attempts to extricate themselves from the harm caused by their products and services, which they do by using a

[10] Dana Priest, "A UAE agency put Pegasus spyware on phone of Jamal Khashoggi's wife months before his murder, new forensics show", *The Washington Post,* December 21, 2021. https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/.
[11] Steven Feldstein and Brian Kot, *Why Does the Global Spyware Industry Continue to Thrive?,* 10.
[12] Craig Timberg et. al., "On the list: Ten prime ministers, three presidents and a king", *The Washington Post*, July 20, 2021, https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.

skewed rhetoric of lawfulness. Firms deem themselves 'lawful' by attaining export licenses from their government for the sale of each product, only taking government entities as clients, and severing contracts with those who they believe are using their products illegally. There is no combination of evidence which supports the idea that an existing spyware firm follows all three of these principles of 'lawfulness' – there is only their word. In fact, there is little publicly available evidence to show how spyware firms operate in any capacity. They rarely reveal who their customers are, and there is no verifiable or record showing if, and how they investigate clients suspected of using their services to commit human rights abuses. Tal Dilian, a well-known figure in the industry,in a 2019 interview, said, "Most of the products that are sold in this industry you cannot monitor. And more than that, customers don't want you to know who their suspects are".[13] Dilian, known for his tracking product, 'Circles', made $21.5 million when Circles and NSO Group were acquired together by US private equity firm Francisco Partners in 2014. Dilian's assertions that firms are largely unable to monitor clients' activities contradicts comments made by Shalev Hulio (founder and former CEO of NSO). In response to The Pegasus Project's reporting, Hulio told the Washington Post that, "Every allegation about misuse of the system is concerning me" and that "It violates the trust that we give customers. We are investigating every allegation…and if we find that it is true, we will take strong action".[14] However, in a separate Washington Post article published a day later, Hulio said that NSO had already "shut off access" to the service for five clients, several years before the Pegasus Project's investigation, after NSO conducted its own 'human rights audit'. He also said that NSO had

[13] Thomas Brewster, "A Multimillionaire Surveillance Dealer Steps Out of The Shadows…And His $9 Million WhatsApp Hacking Van", *Forbes*, August 5, 2019, https://www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/?sh=48d9948331b7.

[14] Elisabeth Dwoskin and Shira Rubin, "NSO Group vows to investigate spyware abuse following Pegasus investigation", *The Washington Post*, July 20, 2021, https://www.washingtonpost.com/technology/2021/07/18/reactions-pegasus-project-nso/.

ended relationships with two additional clients in 2021, before the Pegasus Project went public with their findings.[15] How the clients implicated in The Pegasus Projects' investigation managed to evade detection by NSO's own "human rights audit" has never been explained by the company, but NSO's evasiveness and deflection during press interactions represents the industry's general attitude on human rights – which is that it's is not their problem. This is the kind of firm whose operations expanded to Hungary towards the end of 2017.[16]

What is Lawful Surveillance?

The legality of surveillance is a contested issue, particularly when conducted with Pegasus because it allows for complete, uninhibited access to a device. International recognition of the right to privacy started with Article 12 of the UN's Universal Declaration of Human Rights (1948), which states , "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".[17] While the Universal Declaration of Human Rights (UDHR) is not legally binding, some human rights instruments which derive their principles from UDHR are; one of those treaties is the International Covenant on Civil and Political Rights (ICCPR). Article 17 of ICCPR covers privacy, stating that:

"1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to protection of the law against such interference or attacks."[18]

---

[15] Elizabeth Dwoskin and Shira Rubin, "'Somebody has to do the dirty work': NSO founders defend the spyware they built", *The Washington Post*, July 21, 2021, https://www.washingtonpost.com/world/2021/07/21/shalev-hulio-nso-surveillance/.
[16] Szabolcs Panyi, "The inside story of how Pegasus was brought to Hungary", *Direkt36*, September 28, 2022, https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/.
[17] George T. Papademetriou, "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry," *Harvard Human Rights Journal,* 36, no. 1(2023): 205, https://journals.law.harvard.edu/hrj/wp-content/uploads/sites/83/2023/06/HLH105_crop.pdf.
[18] UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 177, https://www.refworld.org/docid/3ae6b3aa0.html.].

When this paper refers to illegal surveillance or spyware misuse, it means that Article 17's provisions were broken.

Hungarian Surveillance

Pegasus was not the first spyware product Hungary acquired. Between 2010 and 2015 Hungary spent over € 571,000 on surveillance products from Hacking Team, a now defunct Italian firm[19]. However, little publicly available evidence detailing how Hungary used those products exists. Therefore, this paper will devote its attention solely to Hungary's use of Pegasus spyware on four journalists with confirmed infections: Szabolcs Panyi, Andras Szabo, Brigitta Csikasz, and Daniel Nemeth.

Szabolcs Panyi, an investigative reporter for Direkt36, an independent Hungarian news outlet. His areas of focus include national security and defense. After the Pegasus Project's findings went public, forensic analysts from Amnesty International tested Panyi's phone, and found that it had been infected with Pegasus several times, between April and December 2019.[20] The phone of Andras Szabo, Panyi's colleague, had also been compromised by the spyware – twice in 2019. At the time, Szabo was publishing stories on corruption within business and government.[21] Daniel Nemeth, a photojournalist, who documents the lives of Hungary's wealthiest cronies, had Pegasus infections on both of his mobile devices in July 2021, while he was documenting a vacationing Lorinc Meszaros; a former gas fitter, Meszaros started his business empire when childhood friend Viktor Orban, came to power, and is now one of the richest men in the country.[22] Brigitta Csikasz, who is one of Hungary's 'most experienced crime

[19] "Hungary's Orbán government invests in spying technology for use abroad", *Hungarian Free Press*, July 9, 2015. https://hungarianfreepress.com/2015/07/09/hungarys-orban-government-invests-in-spying-technology-for-use-abroad/.
[20] "Szabolcs Panyi", *Forbidden Stories*, 2023, https://forbiddenstories.org/journaliste/szabolcs-panyi/.
[21] Andras Szabo, "Andras Szabo, Hungarian Journalist", Organized Crime and Corruption Project, July 18 2021. https://www.occrp.org/en/the-pegasus-project/andras-szabo-hungarian-journalist.
[22] Stephanie Kirchgaessner, "Phones of journalist who tracked Viktor Orban's childhood friend infected with spyware", *The Guardian,* September 21, 2011,

reporters', with a focus on corruption, was surveilled by Pegasus for a prolonged period of time – April to November 2019.[23]

Pegasus has changed the way journalists work. Szabolcs Panyi stopped using technology to work on projects that involve highly sensitive information. Panyi stated in an interview that,

> "I'm not typing down anything on my computer anymore that's more sensitive. My short-term memory has not been good, historically…But right now I feel that since I store all the information offline in handwritten notes, this is in one word, overwhelming, but this is the only way until I figure out an entirely safe method of how I can store my information digitally. Until then, I just have to rely on these notebooks, and also I'm more mindful of where I bring my phone".[24]

The circumstances which likely motivated the Hungarian government to surveil these four journalists with Pegasus, at various times through 2019 to 2021, will be explored in the main case section of this paper.

Literature Review

Despite the amount of attention Pegasus has received over the course of the last decade, there is not extensive, peer-reviewed scholarship on how spyware is weaponized by governments. Instead, writings on the subject are practically oriented toward exploring solutions to prevent spyware's complicity in human rights violations, and come mainly from journals, foundations, and think tanks.

An overview of the growth of the commercial spyware industry through an international lens can be found in The Carnegie Endowment for International Peace's report, "Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses" produced

---

https://www.theguardian.com/news/2021/sep/21/hungary-journalist-daniel-nemeth-phones-infected-with-nso-pegasus-spyware.

[23] Szabolcs Panyi and Andras Petho, "Hungarian journalist reporting on corruption surveilled with Pegasus for months", *Direkt36*, August 2, 2021. https://www.direkt36.hu/en/honapokon-at-megfigyeltek-pegasusszal-egy-korrupcios-ugyeken-is-dolgozo-magyar-bunugyi-ujsagirot/.

[24] Leila Katibah, "The Politics of Pegasus Spyware: Examining the Impact of Surveillance on Journalism" (Undergraduate Thesis, University of California, Santa Barbara, 2023), 67, https://escholarship.org/uc/item/02k620g6.

by Steven Feldstein and Brian Kot (March 2023). Carnegie's 'Global Inventory of Commercial Spyware and Digital Forensics Technology' tracks government spyware usage: from 2011 to 2023, their database shows at least thirty of the seventy-four government clients (made up of agencies such as police and intelligence services) who bought spyware and other digital forensics technology were either electoral or liberal democracies. Each client (country) is listed along with their regime type, the firm which sold them the surveillance technology, and what the client used the product for. Evidence such as invoices reflecting government payments to firms for a surveillance product, is used to substantiate relationships between clients and firms. Carnegie's report considers the European Union an enabling force in the growth of the spyware industry. Feldstein and Kot found that EU states approved the export of surveillance technology 317 times between 2015 and 2017, while rejecting just fourteen applications[25].

In terms of reducing government abuse of spyware at an international scale, the Feldstein and Kot put that responsibility solely in the hands of democratic governments, and assert that the most realistic and effective approaches would be to require that spyware firms do not sell their software to clients with the worst human rights records and compel firms to incorporate mandatory human rights due diligence requirements[26]. Feldstein and Kot suggest, as a starting point, that Europe, Israel and the United States become more cooperative with each other and maintain unified registries of cyber surveillance firms, in order to stop the common practice amongst firms of hiding the details of their ownership within complex corporate structures[27]. Speaking directly to the United States government, Feldstein and Kot propose a shift towards multilateralism by putting pressure on European Countries to implement the US Entity List (which prevents spyware firms like NSO Group and Candiru from buying US technologies). In

[25] Steven Feldstein and Brian Kot, *Why Does the Global Spyware Industry Continue to Thrive?,* 7.
[26] Ibid, 8.
[27] Ibid, 9.

terms of what the US shouldn't be doing, the Feldstein and Kot cite recently ramped up partnerships with countries in the intelligence and cybersecurity fields who have committed human rights abuses with surveillance technologies: the January 2023 announcement by the Biden administration of its intentions to include Bahrain, Morocco, and the UAE on cyber-defense collaborations is considered an example of US permissiveness towards spyware misuse, because all three countries have targeted government critics and journalists with spyware[28].

The Lawfare Institute, in partnership with the Brookings Institution published Asaf Lubin's paper, "Regulating Commercial Spyware" (2023), where he explains what he perceives are four failed methods of regulation – industry self-regulation, ad hoc litigation, ex post blacklisting and sanctions – and why they have failed, followed by his proposal for a new, multi-stakeholder framework, the Commercial Spyware Accreditation System (CSAS). The first failed method is industry self- regulation: Lubin asserts that self-regulation is difficult for any industry because, "Firms lack sufficient incentives to set, comply with, police and punish violations of their own standards, and markets cannot ensure that firms will behave with integrity."[29] In Lubin's eyes, the expectation that the spyware industry – which is already prone towards complicity in human rights abuse – will somehow overcome these challenges, is an expectation not based in reality. The second method, ad-hoc litigation will likely fail because laws have not been able to adequately distinguish who carries legal responsibility in the commission of spyware crimes – whether that be private entities or foreign sovereign entities (who are able to claim sovereign immunity in some countries), as well as the fact that spyware

[28] Ibid, 25.
[29] Asaf Lubin, *Regulating Commercial Spyware*, (Washington, DC: The Lawfare Institute, August, 2023): 19, https://www.lawfaremedia.org/article/regulating-commercial-spyware.

operates largely in secret, which hinders a petitioner's ability to collect evidence for a given case.[30]

As to the effectiveness of blacklisting, Lubin points out that the US' decision to blacklist NSO in 2021, failed to make meaningful improvements to the behavior of the spyware industry as a whole. While NSO's bottom-line was hurt after being put on the Entity List, the company continues to operate today[31]. Aside from these failed methods of regulation, Lubin also questions proposals for a spyware moratorium, which he calls, a "disingenuous" solution for two reasons: one, commercial spyware offers a needed solution to law enforcement in order to protect society in the digital age, and two, without the availability of spyware as a targeted solution, government would likely pressure providers of internet-based services to design backdoors in their products.[32] Backdoor access enables one to bypass a provider's existing security system, which would make abuse of privacy rights easier, and stifle the security innovation needed to deal with authoritarian countries who would likely not comply with a moratorium .[33]

Lubin advocates for a holistic regulatory approach, with the creation of a 'multistakeholder standardization and accreditation model' as a solution, which he calls the Commercial Spyware Accreditation System (CSAS)[34]. The framework would be a binding international agreement, with signatories consisting of national government and firms. Once signatories are vetted and accepted, membership would remain conditional on continued compliance with strict human rights standards. A board of directors would be elected by the members of the framework, and the board would likely consist of those who have worked in the industry or who have been members of civil society organizations; their responsibilities would

[30] Ibid., 10.
[31] Ibid., 21.
[32] Ibid., 22.
[33] Ibid., 23.
[34] Ibid, 26.

include reviewing requests to join the agreement, as well as reviewing and deciding appeals in grievance cases brought against a participating company.[35] National Contact Points (NCPs), would be elected for each participating country, and would be responsible for handling grievances brought to CSAS in their respective country through services such as confidential mediation between conflicting parties. According to Lubin, NCPs would most likely have past experience in the spyware industry as well as security clearance. Their job would also include enhancing the functioning of CSAS through dialogue with NCPs from other countries, in addition to proposing model language for standard contracts between governments and spyware firms. Lubin used concepts from the Organization for Economic Cooperation and Development Guidelines for Multinational Enterprises (OECD MNE Guidelines) to create his NCP model.[36]

Lubin's framework would require companies no longer be able to keep zero-days a secret, a key component of spyware architecture. The utility of zero-days in the creation and deployment of spyware will be explained in detail in the main case section of this paper, but for the purpose of understanding Lubin's framework, the basic definition will suffice: "A zero-day exploit is a cyberattack vector or technique that takes advantage of an unknown or unaddressed security flaw in computer software, hardware or firmware. 'Zero day' refers to the fact that the software or device vendor has zero days, or no time, to fix the flaw, because malicious actors can already use it to gain access to vulnerable systems".[37] Some countries already regulate governmental hoarding of zero-days through something called a Vulnerable Equities Process (VEP) which, "outlines the procedure through which the government weighs various considerations in determining when to disclose software vulnerabilities and when to exploit them for law enforcement or foreign intelligence purposes. Disclosure enables the involved company

[35] Ibid, 29
[36] Ibid, 30.
[37] IBM, "What is a zero-day exploit?,"accessed December 13th, 2023, https://www.ibm.com/topics/zero-day.

or entity to patch for that vulnerability and protect users' cybersecurity".[38] Lubin argues that VEPs are currently ineffective because they do not force spyware firms to join in on the process, making it possible for governmental agencies to circumvent governmental regulation by buying commercial spyware.[39] CSAS would ban the privatization of zero-day exploits, and would require spyware firms to receive the consent of their respective governments to exploit a freshly discovered zero-day vulnerability in the development phase of their product.[40]

In "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Industry" (2023), George Papademetriou identifies two major causes behind governments now utilizing spyware firms for surveillance technology: the first is global adoption of cell phones, which are rich sources for personal information. The second is that in the post-Snowden era, deployment of end-to-end encryption by companies handling the transfer of internet data has become a norm rather than a rarity.

To better understand how different policy choices could reduce the spyware industry's general ability to enable abuse (rather than focusing on a single firm like NSO), Papademtriou employs a framework created by Law Professor and political activist, Lawrence Lessig. The framework (henceforth referred to as Lessig's Four Constraints), was first introduced in Lessig's article "The New Chicago School" (1988), and developed further in his book, *Code 2.0* (2006).[41] A useful method for "analyzing regulation in cyberspace", Lessig's Four Modalities of Regulation (henceforth Lessig's Modalities) frames the regulatability of the internet through four interdependent spheres, 'constraints': law, norms, architecture, and market:[42] Law, at its core, "directs behavior in certain ways". The state creates rules, and imposes penalties for breaking

[38] Lubin p. 27
[39] Lubin p. 28
[40] Lubin p. 32
[41] Papademetriou, "Disrupting Digital Authoritarians", 201.
[42] Ibid., 202.

those rules in order to influence how people will behave. Norms depend on community internalization and enforcement by shunning or condemning those members who violate socially acceptable behavior. Markets influence behavior through prices, which are governed by the relationship between supply and demand. Architecture refers to code and hardware, which come together to form the pathways which govern a user's ability to execute certain actions.

The overall effect or success of regulation is the sum of Lessig's four constraints.[43]

Papademetriou chooses to explore two of the modalities, markets and laws, as opposed to all four, for policy solutions:

> "though cataloguing and assessing possible developements across all four four vectors may be possible in theory, a narrower analysis of a subset of relationships allows for more concrete and actionable insights…while architecture – including physical teleommunications infrastructure, internet routing protocols, and end-user devices like laptops and cell phones – plays a crucial role in the surveillance ecosystem, it is a mode of regulation that is both constantly evolving and difficult to modulate. Leading scholars have noted shifts in the architecture of the internet…these developments are important for the future of privacy but offer more problems than solutions".[44]

Of the possible policy arenas which can impact markets through law, Papademtriou surveys recent developments in international human rights instruments, export control regimes and criminal sanctions, and civil litigation.

Papademetriou says that the UN's framework for privacy rights must be supplanted by new "authoritative interpretations" of the right to privacy to better reflect the changing technological landscape. Papademetriou asserts that firms are increasingly responsive to reputational costs, and that stronger and clearer norms regarding privacy will make the reputational costs of failing to comply more obvious to firms, and more useful as a means of enforcement. One possible, and already existing mechanism for enforcement is the UN Guiding Principles on Business and Human Rights (UNGPs), which Papademetriou thinks could be more

[43] Ibid., 203.
[44] Ibid., 204.

effective if the document were revised to include more stringent language on surveillance technology.[45]

While addressing the current state of export control regimes and criminal sanctions, Papademetriou zeroes in on the role of the United States, because of its market size and outsized role in the functioning of the global financial system. He praises the ramping up of export control regulation during the Biden administration, and the first additions of spyware firms to the Entity List (which limits their access to technology originating from the U.S.), but condemns past politicization of these controls ,which penalize some firms and not others, despite being guilty of the same types of crimes.[46] The significant financial power of the US, in conjunction with strong state capacity, are two facts Papademtriou uses to predict that countries who share democratic values (i.e. European ones), will be less willing to buy products from the U.S.-sanctioned firms because of the risk to trade relationships and other political benefits tied to maintaining good U.S. relations.[47]

Papademetriou points out possible paths for civil litigation, and focuses predominantly on the U.S. legal system. He asserts that The Alien Tort Statute is not a particularly viable tool for non-citizens to make claims against spyware firms (corporate defendants) because of extraterritoriality exclusions. Papademtriou feels more confident in the utility of The Computer Fraud and Abuse Act (CFAA), because it can be applied to extraterritorial cases, but he also notes that it still faces complicated jurisdictional issues. Papapdemtriou also points out that The Foreign Sovereign Immunity Act (FSIA), stands in the way of holding sovereign governments accountable for their complicity in privacy violations.[48] Lastly, Papademetriou addresses issues

[45] Ibid., 209.
[46] Ibid.
[47] Ibid., 212.
[48] Ibid., 217.

of causation. In order for plaintiffs to prove they have standing to bring a claim, they must be able to assert causation, linking the actions of a firm to the crime committed, which Papademetriou thinks will be difficult. In his eyes, thorough forensic analysis can prove causation, but lack of access may be the biggest obstacle for the majority of victims who wish to hold firms accountable.[49]

Papademtriou concludes by suggesting that regulators will be most successful if they use a combination of policy measures – and that a successful path forward:

> "(1) clarifies international human rights obligations that arise from the right to privacy, (2) bases export control regimes on multilateral consensus and recognized principles of human rights law, and (3) expands opportunities for civil litigation in domestic courts."[50]

Papademetriou acknowledges that changing international human rights obligations will be a challenge, but even if the international legal landscape pushes back, gains can nonetheless be made through the byproduct of consensus building – the fortification of norms. He also asserts that export controls and sanctions are effective weapons against spyware firms' bottom-line, but the US' inconsistent application of these tools threatens to undermine opportunities to improve human rights standards within the country, and elsewhere. In terms of civil litigation, he concludes with two recommendations: one, that the Computer Fraud and Abuse Act is a law that could be useful for plaintiffs in the future, so long as the judiciary rules in their favor on unresolved extraterritoriality and jurisdictional issues, and two, that the government should provide more resources to victims of illegal spyware surveillance so as to help these people legally attribute causation bad actors.[51]

[49] Ibid., 218.
[50] Ibid., 220.
[51] Ibid., 221.

Methods

This project contextualizes Hungary's surveillance of journalists from 2019 to 2021 by investigating how regulatory forces, particularly those related to Hungary's membership in the EU, failed to prevent the surveillance from occurring. It applies Papademetriou's (2023) approach, and Lessig's (2006) Four Modalities framework (laws, markets, architecture, and norms, by moving through each of the 4 in turn. Examining laws involved close reading of Hungary's law on secret surveillance, and challenges brought against the law in the European Court of Human Rights. To consider Lessig's second category of Markets, the project had to work around lack of information, like product pricing, which would otherwise be available for ordinary products. However, the work of investigative journalists allowed for some insight into how much money some countries have spent on Pegasus, including Hungary. In the absence of available records from Hungary, US reports on the cost of wiretapping operations enabled a cost comparison between spyware and alternative means of surveillance. In terms of architecture, reports by institutions dedicated to forensic analysis of spyware infections and operations, like Citizen Lab, provided information on the architectural features of Pegasus, and Hungary's use of it. The UN's various human rights instruments regarding privacy, in addition to looking at the US' recent and current initiatives to combat the use of spyware for illegal purposes, were used to establish states' current understanding of norms regarding privacy, and how the use of spyware may, or may not depart from those norms.

Investigating the Use of Pegasus in Hungary

Laws

Law has the ability to direct behavior in cyberspace through penalties, i.e. by punishing an agency who uses spyware illegally; but it does not always do so effectively, if at all.[52] A case from the mid 2010s, which was litigated in both Hungary's courts and the European Court of Human Rights (EUCtHR), sheds light on how Hungary's legal system was primed to enable arbitrary surveillance before spyware even came into the picture. The case also demonstrates that international courts are limited in their ability to direct state behavior.

In the case of Szabo and Vissy v. Hungary (henceforth Szabo and Vissy), the EUCtHR found that a portion of a Hungarian surveillance law violated privacy rights enumerated by Article 8 of the European Convention on Human Rights. Article 8 states that:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[53]

The case started in Hungary in 2011, and went all the way up to the Hungarian Supreme Court before the plaintiffs brought their case to the EUCtHR in 2014. The NGOs Privacy International, and the Center for Democracy and Technology both filed submissions for the case in support of the plaintiffs, Mate Szabo and Beatrix Vissy, who at the time were both employees of Eotvos Karoly Koszpolitikai Intezet (EKINT), also an NGO.[54]

---

[52] Lawrence Lessig, *Code 2.0,* (New York: Basic Books, 2006), 124.
[53] European Court of Human Rights, *Guide on Article 8 - Right to respect for private and family life, home and correspondence*, (Strasbourg: August 8, 2022), 7. https://www.echr.coe.int/documents/d/echr/guide_art_8_eng.
[54] Case of Szabó and Vissy v. Hungary, 37138/14, HUDOC, EUCtHR 4th Section, (January 12, 2016). https://hudoc.echr.coe.int/eng?i=001-160020.

According to Szabo and Vissy's filing to the Hungarian Constitutional Court and the EUCtHR, their employer functioned as a government "watchdog".[55] EKINT, founded in 2003 by the Soros Foundation, "seeks to establish a novel, unconventional institutional framework for shaping democratic public affairs in Hungary", according to its website, and "wishes to contribute to raising professional and general public awareness and to shaping the political agenda in issues with an impact on the quality of relations between citizens and public power".[56] Szabo and Vissy worried that Orban's government might violate their privacy through secret surveillance, and their fears were not unfounded.

Far-right nationalists started targeting the founder of EKINT, George Soros, in the nineties. Soros, a Hungarian-born billionaire, was accused in 1992 of being a part of a Jewish conspiracy to suppress Hungary's post-Communist development; Istvan Csurka, who was the vice president of the Hungarian Democratic Forum party at the time, called Soros a "puppet of Jerusalem".[57] Viktor Orban, appropriated this narrative when he became Prime Minister in 2010, and brought it to a head in 2017, when he launched a national television and billboard campaign that blamed Soros for an influx of Middle Eastern migrants.[58] A proponent of liberal democracy, and 'open societies', Soros founded The Central European University in Budapest in 1991. Orban's government pushed the university out of Hungary in 2018 despite its reputation as one of the best schools in the region.[59]

---

[55] Ibid.
[56] Eotvos Karoly Intezet, "Introduction", 2015, https://www.ekint.org/en/about.
[57] Peter Maas, "U.S. Interests Try to Counter Hungarian Rightist", *The Washington Post,* October 20, 1992, https://www.washingtonpost.com/archive/politics/1992/10/20/us-interests-try-to-counter-hungarian-rightist/ed26f474-a87f-4770-b27b-eff89aadba72/.
[58] Lydia Gall, "Hungarian Government Stoops to New Low with Hate Campaign", *Human Rights Watch,* July 12, 2017. https://www.hrw.org/news/2017/07/12/hungarian-government-stoops-new-low-hate-campaign.
[59] Shaun Walker, "Dark Day for freedom': Soros-affiliated university quits Hungary". *The Guardian*, December 3, 2018.
https://www.theguardian.com/world/2018/dec/03/dark-day-freedom-george-soros-affiliated-central-european-university-quits-hungary

When Szabo and Vissy first brought their case to Hungary's courts in 2011, the country was undergoing monumental political and governmental change. Viktor Orban had become Prime Minister for the second time the prior year (his previous tenure lasted only 4 years, from 1998 to 2002), and his right-wing party Fidesz won a supermajority in the Hungarian parliament. By 2012, Fidesz managed to make significant changes to Hungary's legal framework, including the passage of a new constitution, called 'the Fundamental Law'. A 2013 report published by Human Rights Watch concluded that the changes made by Fidesz, "weaken legal checks on its [Fidesz] authority, interfere with media freedom, and otherwise undermine human rights protection in the country".[60] Szabo and Vissy had valid reason to fear that their right to privacy might be infringed with Orban in power.

Szabo and Vissy challenged parts of Hungary's surveillance law, as amended in 2011.[61] The amendment, Act no. CCVII of 2011 (called the "Police Act"), delineates how the TEK determines the kinds of acts or behaviors which merit targeted surveillance, in addition to how the TEK should acquire authorization for carrying out such operations.[62]

In their application to the EUCtHR, Szabo and Vissy claimed that 'section 7/E (3)', which explains the authorization process for "secret surveillance within the framework of intelligence gathering for national security" violated their rights under Article 8 of the European Convention on Human Rights. Under Hungarian law, there are two different sets of rules for secret surveillance operations; which rules govern an operation is an important distinction, and depends on what kind of crime or activity is being monitored. 'Section 7/E (3) surveillance'

---

[60] Human Rights Watch, *Wrong Direction on Rights: Assessing the Impact of Hungary's New Constitution and Laws,* May 16, 2013, https://www.hrw.org/report/2013/05/16/wrong-direction-rights/assessing-impact-hungarys-new-constitution-and-laws.

[61] The surveillance law is Act no. XXIV of 1994 on the Police;
Case of Szabó and Vissy v. Hungary," The Facts", Sec. 1.

[62] The TEK, (Terrorelhárítási Központ), is Hungary's Anti-Terrorism Task Force, established in 2010.

concerns surveillance in the interest of national security, can be used to investigate terrorist attacks, and is the subject of Szabo and Vissy's complaint. The other framework, spelled out in 'section 7/E (2) surveillance', requires judicial authorization and is "conditional on the suspicion of certain serious crimes", meaning that it is "always linked to a particular crime and could only be ordered for the purposes of identifying or locating suspects", whereas 'section 7/E (3)' surveillance is not subject to judicial review, does not need a particular crime and only needs the authorization of one person – the Minister of Justice.[63]

While '7/E (2)" requires detailed reasoning for its use for judicial review– '7/E (3)' does not require the minister's reasoning prior to authorization, since he is the only decision maker involved. Furthermore, when TEK asks the Minister of Justice to extend the 90-day time frame for surveillance under '7/E (3)', the Minister is not entitled to know the results of the surveillance operation for which he is being asked to make an extension for. Lastly, data that is collected but irrelevant to a crime being investigated under '7/E (2) surveillance' must be destroyed within eight days, while there are no obligations for destroying data collected during '7/E (3) operations'[64].

The kinds of activities which fall under the '7/E (3)' umbrella are defined in Section 74(a) of the law, and those which fall under the interest of national security, i.e. 7/E (3) are listed under five subsections. One section refers directly to terrorism, while another is less specific, naming, "efforts violating or threatening the political, economic or defense interests of the country", as worthy of '7/E(3)'. While the EUCtHR did not oppose the broad language of what constitutes a national security threat under Hungarian law, "national authorities enjoy a certain amount of margin appreciation", they did take issue with the loose content requirements for the

[63] Case of Szabó and Vissy v. Hungary (2016), "The Facts", Sec. 1.
[64] Ibid.

motions which agencies must submit to the Minister of Justice in order to obtain permission to start a new '7/E(3)' surveillance operation.[65] For instance, the motion must contain only, "the premises of the secret intelligence gathering, the person(s) concerned identified by name or as a range of persons, and/or any other information capable of identifying such person or persons".[66] The court found that, "the category is overly broad, because there is no requirement of any kind for the authorities to demonstrate the actual or presumed relation between the persons or range of persons "concerned" and the prevention of any terrorist threat – let alone in a manner enabling an analysis by the authoriser which would go to the question of strict necessity".

Overall, the Court decided that 7/E(3)'s lack of judicial oversight made the risk for arbitrary use too great. In addition, the fact that citizens had no means of seeking redress was considered a problem, since no part of the law required they be notified that surveillance had occurred once the operation had completed. For those reasons the Court found the law in violation of Article 8 of the European Convention on Human Rights.

The ruling did not go as far to protect citizens from arbitrary invasion of privacy as Szabo and Vissy probably hoped. Since the Court's ruling, Hungary has not revised the law to require judicial authorization for secret surveillance in place of the prerogative of a single person, the Minister of Justice. The PEGA Committee conducted a fact-finding mission, and spent an hour with two key officials, Mr. Zoltan Sas, Chair of the Parliamentary Committee on National

---

[65] Case of Szabó and Vissy v. Hungary, "The Law, B. The Merits, 2. The Court's assessment"..;
"The margin of appreciation is a doctrine that the European Court of Human Rights has developed when considering whether a member state has breached the Convention. It means that a member state is permitted a degree of discretion, subject to Strasbourg supervision, when it takes legislative, administrative or judicial action in the area of a Convention right. The doctrine allows the Court to take into account the fact that the Convention will be interpreted differently in different member states, given their divergent legal and cultural traditions. As the Council of Europe has observed, the margin of appreciation gives the Court the necessary flexibility to balance the sovereignty of member states with their obligations under the Convention".
"Margin of Appreciation", Open Society Justice Initiative, April 2012",
https://www.justiceinitiative.org/uploads/918a3997-3d40-4936-884b-bf8562b9512b/echr-reform-margin-of-appreciation.pdf.

[66] Case of Szabó and Vissy v. Hungary, "The Law, B. The Merits, 2. The Court's assessment".

Security and Mr Istvan Simikco (former Minister of Defense). Zoltan Sas had been a member of the committee for eleven years prior to taking over the chairmanship in the spring of 2022.[67] When asked about the Committee on National Security's investigations of complaints regarding secret surveillance Mr. Sas replied, "As for the complaints that we received, we investigated these complaints. And what we could say after this investigation is that the pro forma rules were observed. But again, we were not allowed to look deeper into the investigation, for example, into whether their privacy was violated or not."[68]The fact that someone on the committee tasked with investigating complaints regarding secret surveillance felt that they had satisfied their job without being able to determine whether someone's privacy had been violated or not demonstrates that Hungary's domestic laws, left unchecked, essentially granted the government permission to abuse spyware.

Markets

The foundational concept for Lessig's market modality is prices . To determine how price considerations played into Hungary's decision to buy Pegasus, first the price of an alternative more traditional means of surveillance must be established. What was a form of surveillance Hungary likely relied on prior to upgrading to Pegasus? Wiretapping. However, statistics for Hungary's wiretapping operations are not available, so this paper evaluates publicly available statistics from the United States in order to make general inferences about wiretapping operations, so that a cost-benefit analysis can be made between more traditional methods of targeted surveillance (i.e. wiretapping) and spyware.

[67]PEGA Committee, *Mission Report: following the mission to Hungary – 20 and 21 February 2023.* Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware, April 20, 2023, https://www.europarl.europa.eu/doceo/document/PEGA-CR-746829_EN.pdf
[68] Ibid. Page 9.

The United States Courts' Wiretap Reports contain statistics for wiretaps that were authorized by federal and state court judges for the year. In 2021, 2,245 wiretaps were authorized, and over half of those wiretap authorizations (1,289) included cost data[69]. The average cost of a wiretap as reported for federal and state court authorizations was $161,818, and the average length of a wiretap operation was 44 days. The number of state wiretaps which encountered encryption decreased from 184 in 2020 to 176 in 2021, but of those 176, state officials were only able to decipher the plain text of messages for 5 cases. 183 federal wiretaps encountered encryption and only 22 could be decrypted[70]. If the US government were to use software like Pegasus (which would be illegal under US law, and so far there is no evidence that it has been used for actual surveillance operations), then the barrier of encryption would likely go away. By comparison, the Hungarian Minister of Justice authorized 1,038 permits for secret information gathering in 2015; that number has subsequently risen to 1,200-1,300 permits per year – at least. In the first three months of 2021, nearly 500 permits were issued[71]. While the U.S. was – at most – authorizing double the amount of permits for our wiretapping and Foreign Intelligence Surveillance operations, the U.S. population in 2021 was more than 34 times that of Hungary's, showing that Hungary far outpaces our propensity for wiretapping. If wiretaps were doled out at random in 2021, one's chances of being targeted in the US would be 1 out of 147,884 people in the US versus 1 out of 19,420 in Hungary.

Now to see how the cost of wiretapping compares to its much more advanced replacement, information must be found on Pegasus' price. The secretive nature of Pegasus

---

[69] Administrative Office of the U.S. Courts, *Wiretap Report 2021*, United States Courts, December 31, 2021, https://www.uscourts.gov/statistics-reports/wiretap-report-2021.
[70] Ibid.
[71] Szabolcs Panyi and Andras Petho, "Hungarian journalists and critics of Orban were targeted with Pegasus, a powerful Israeli cyberweapon", *Direkt36,* July 19, 2021, https://www.direkt36.hu/en/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/.

makes ascertaining the cost of its use for long durations nearly impossible. However, investigative journalists have produced enough evidence to give us snapshots into what that cost has been at various times. Nicole Perlroth, who spent a decade as the NY Times lead reporter on cybersecurity, and now serves as an adviser to the Department of Homeland Security and Infrastructure Security Agency (CISA), wrote about one of NSO's commercial proposals for the Pegasus system back in 2016. At the time, NSO priced their 'flat installation fee' at $500,000, with the cost of tracking 10 iPhone users set at $650,000 (the price for 10 Android users was the same). The price of additional users was set at a sliding scale which topped out at $800,000 for 100 additional targets. NSO also charged an annual service fee of 17 percent of the total cost[72]. At minimum it would have cost a buyer $1,150,000 for one year of access to Pegasus. To adjust for inflation, that would be $1,298,360.85 in 2021. For that price a government could have unlimited access to the phones of 10 targets for a year at an average cost of $129,836.085 while traditional wiretapping in the U.S. cost the government an average of $161, 818 for an average length of 44 days, making Pegasus an economical alternative to wiretapping.

In 2021, the chairman of the Hungarian parliament's Committee on Defense and Law Enforcement, Lajos Kosa, confirmed to journalists that Hungary's Interior Ministry had bought Pegasus[73]. One of the Hungarian journalists whose phone had been infected by Pegasus, Szabolcs Panyi, found in the process of his own investigation that the Hungarian government approximately 6 million euros to acquire Pegasus at some point between 2017 and 2018, and that they would have been able to monitor as many as 50 phones[74].

---

[72] Nicole Perlroth, "How Spy Tech Firms Let Governments See Everything on a Smartphone", *New York Times*, September 2, 2016, https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html.

[73] Justin Spike, "Hungarian official: Government bought, used Pegasus spyware", *AP News,* November 4, 2021, https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0.

[74] Panyi, Szabolcs. "Boosting of Spying Capabilities Stokes Fear Hungary Is Building a Surveillance State", *Balkan Insight*, October, 23, 2022,

How much of that 6 million translated directly into cost-per-target is an unanswered question, some of it had to have gone to the training received by Hungarian surveillance operatives to be able to use Pegasus software; however, it does allow us to see that while the spyware would come at an incredible cost to a normal individual, the benefits far outweigh the costs, at least monetarily speaking, for government usage. To put into perspective how much other governments are willing to spend on the software, Pegasus spyware was first sold to Saudi Arabia in 2017 for 55 million dollars.[75] Mexico's top security official told the press in 2021 that the two previous administrations spent a combined 300 million dollars on spyware and surveillance purchases, of which 61 million dollars went to Pegasus[76]. Hungary's contract for 6 million euros is inexpensive when compared to those numbers. Beyond the reasonable pricing, what did the Hungarian government hope to achieve with their investment? An answer may be found in the country's relationship with the EU, which was splintering.

The passage of a new Hungarian constitution in 2011 - the Fundamental Law- brought the quality of democracy, and whether Hungary was abiding by rule of law principles into greater question. In 2015, European Parliament passed resolutions reflecting concerns about the decline of liberal democratic values – once in June, and a second time in December[77]. The European Parliament passed a third resolution in the spring of 2017, which made explicit concerns about how Hungary responded (or did not respond) to the European Court of Human Right's ruling in

---

https://balkaninsight.com/2022/10/13/boosting-of-spying-capabilities-stokes-fear-hungary-is-building-a-surveillance-state/.

[75] MEE Staff, " Pegasus: MBS called Netanyahu to renew Saudi Arabia's NSO license, report says. January 28, 2022, https://www.middleeasteye.net/news/pegasus-saudi-arabia-mbs-called-netanyahu-renew-nso-spyware-license-report-says.

[76] "Mexico says officials spent $61 million on Pegasus spyware", Mexico City AP, July 18, 2021, https://www.pbs.org/newshour/world/mexico-says-officials-spent-61-million-on-pegasus-spyware.

[77] European Parliament, "European Parliament resolution of 10 June 2015 on the situation in Hungary" (2015/2700(RSP)) June 10 2015, https://www.europarl.europa.eu/doceo/document/TA-8-2015-0227_EN.html; and European Parliament "European Parliament resolution of 16 December 2015 on the situation in Hungary" (2015/2935(RSP)) December 16, 2015 https://www.europarl.europa.eu/doceo/document/TA-8-2015-0461_EN.html.

Szabo and Vissy, "whereas in the case of *Szabo and Vissy v. Hungary* the European Court of Human Rights ruled that Hungarian legislation on secret anti-terrorist surveillance introduced in 2011 had been a violation of the respect for private and family life, home and correspondence"[78].

The European Parliament kicked the pressure up a notch in September 2018, by passing a resolution that called on the EU Council to "determine, pursuant to Article 7(1) of the Treaty on European Union, the existence of a clear risk of a serious breach by Hungary of the values on which the Union is founded[79]. Article 7(1) allows the European Council to give a formal warning to member states who are found to have committed fundamental rights violations[80]. In the resolution, Parliament stated the following areas of concern regarding Hungary :

> "The functioning of the constitutional and electoral system; The independence of the judiciary and of other institutions and the rights of judges; Corruption and conflicts of interest; Privacy and data protection; Freedom of expression; Academic freedom; Freedom of religion; Freedom of association; The right to equal treatment; The rights of persons belonging to minorities, including Roma and Jews, and protection against hateful statements against such minorities; The fundamental rights of migrants, asylum seekers and refugees; Economic and social rights".[81]

Finally, in 2022, a conditionality mechanism for the protection of the EU budget, was put into effect against Hungary. The mechanism first became a part of EU law the previous year, and allows the EU to suspend funding for member states found to be breaching rule of law principles, and is separate from Article 7 proceedings[82]. However, the new law added a needed means of force to push Hungary into compliance, which Article 7 lacked . Article 7 has the capability to severely handicap a country politically by stripping their right to vote in the EU Council.

---

[78] Europen Parliament, " European Parliament resolution of 17 May 2017 on the situation in Hungary" (2017/2656(RSP))May 17, 2017 https://www.europarl.europa.eu/doceo/document/TA-8-2017-0216_EN.html.
[79] European Parliament, "European Parliament resolution of 12 September 2018" (2017/2131(INL)) September 12, 2018, https://www.europarl.europa.eu/doceo/document/TA-8-2018-0340_EN.html#def_1_2.
[80] Ginger Hervey and Emmet Livingstone, "What is Article 7?", *Politico,* January 13, 2016. https://www.politico.eu/article/hungary-eu-news-article-7-vote-poland-rule-of-law/
[81] European Parliament, "European Parliament resolution of 12 September 2018".
[82] EU Commission, "Rule of law conditionality regulation", 2022. https://commission.europa.eu/strategy-and-policy/eu-budget/protection-eu-budget/rule-law-conditionality-regulation_en

However, in order to do so a unanimous vote must be brought against the concerned country in order to remove the right. Hungary has been able to block such a measure from occuring by forming an alliance with Poland, who is also undergoing Article 7 proceedings[83]. But Hungary would lose part of its access to the budget.

The European Commission told Hungary that the country had triggered the conditionality mechanism in April of 2022[84]. The following December the European Council put in place the Hungarian recovery and resilience plan (RRP), which included 38 measures, 111 milestones and targets, with 27 milestones named as "super-milestones". A briefing published by the European Parliament states the intent behind the super-milestones: "the major areas included are corruption, public procurement, judicial independence and decision-making, most of which featured in the Article 7 procedure and one or more rule of law reports on Hungary"[85]. In addition, the Council decided to withhold €6.3 billion of funds from Hungary. In 2021 Hungary had contributed €1.7 billion to the EU's budget and in turn received €6 billion[86]. Hungary's GDP for 2022 was $178.79 billion[87]. The funds that the EU withheld are equivalent to more than

[83]Jorge Libeiro and Sandor Zsiros," Hungary is no longer a full democracy but an 'electoral autocracy', MEPS declare in new report", *euronews,* updated September 16, 2022, https://www.euronews.com/my-europe/2022/09/15/hungary-is-no-longer-a-full-democracy-but-an-electoral-autocracy-meps-declare-in-new-repor.

[84] The Greens/European Free Alliance. "Rule of Law: Commission Triggering of Conditionality Mechanism Against Hungary Long Overdue." April 27, 2022. https://www.greens-efa.eu/en/article/press/rule-of-law-commission-triggering-of-conditionality-mechanism-against-hungarian-government-long-overdue

[85] Andras Schwarcz, Rule of law-related 'super milestones' in the recovery and resilience plans of Hungary and Poland, *European Parliament, Policy Department for Budgetary Affairs*, January 2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/741581/IPOL_BRI(2023)741581_EN.pdf

[86] Krisztina Koenen, Hungary and the EU: A deepening divide, *GIS Reports*, May 17, 2023. https://www.gisreportsonline.com/r/hungary-eu-divide/.

[87] Hungary. *The World Bank.* https://data.worldbank.org/country/hungary

3.75% of Hungary's GDP for 2022[88]. To put that figure into some perspective, the United States' reported military spending in 2022 was approximately 3.44% of US GDP[89].

Law and Markets Intersecting

How do all of these numbers relate back to Hungary's surveillance on journalists? One could speculate about whether, and if so when, the Hungarian government expected some form of punishment for failing to effectively resolve the concerns raised by the EU. However, it is important to remember that the stories which the journalists with confirmed Pegasus infections were reporting on are all related to the concerns named in the Article 7 Proceedings against Hungary: corruption, judicial independence, media plurality. No information exists publicly which would provide insight into what the Hungarian government aimed to achieve, or felt they *did* achieve by spying on these journalists through the use of Pegasus. However, a valid estimation would be – based on the timeline of the Article 7 proceedings, and the freezing of cohesion investment funds in 2022 – that certain entities within the Orban government had a strong incentive to track these journalists' activities, even if they weren't acting on a hunch for something extremely specific. If Orban can't plausibly get rid of all independent media, then why not make the ones that must remain useful? While none of the journalists were prevented from publishing their stories outright, the government would have had access to all of their personal data and been able to learn who their sources were via Pegasus. So far, no one knows what the government will do – or have done – with the collected data.

When considering the €6 million price of obtaining and using Pegasus, Hungary would have been highly incentivized rather than disincentivized, to buy the spyware. While Hungary

---

[88] The number is 3.77% Exchange rate used was from market close on December 30, 2022. *Pound Sterling Live.* https://www.poundsterlinglive.com/history/EUR-USD-2022.

[89] Result based off of The World Bank's estimate of US GDP for 2022 https://data.worldbank.org/country/united-states?name_desc=false and the Stockholm International Peace Research Institute's reporting of US military expenditure for 2022 at $877 billion in

has been chastised for its treatment of the media, it would be wrong to assume that buying Pegasus to spy on journalists was an unnecessarily risky move, since if it were publicized (as it was), Hungary's crackdown on the media is but one of many issues that have upset the EU.

Architecture

The architectural features of Pegasus' code, which make it so formidable in the hands of surveillance operatives, and so repellant to regulation suited for the physical world, were brought to a new level of distinction sometime between Pegasus' release in 2013 and the summer of 2016.[90] That summer, Citizen Lab was able to determine that NSO had managed to program the software in such a way that it could download itself by remotely 'jailbreaking' an iPhone; "to jailbreak means to modify a device, usually a smartphone, by removing any restrictions imposed by the device manufacturer, such as the downloading and installation of unauthorized software or apps from third-party markets"[91]. Some people choose to jailbreak their iPhone in order to download apps that are not found in the Apple app store, which the design of iOS (iPhone operating system) does not allow. While jailbreaking a phone allows for greater personalization of a phone, doing so also eliminates layers of security, can cause the phone to crash, disrupt cellular data and the functionality of other apps, and shorten battery life. Depending on how the phone is modified, it can become inoperable should the user try to install updated iOS software[92].

Citizen Lab encountered this version of Pegasus while conserving with Ahmed Mansoor, an internationally renowned and awarded human rights lawyer, who is also a citizen and resident of the UAE[93]. This would become the third time that Mansoor had been targeted with

---

[90] Bill Marczak and John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" Citizen Lab, August 24, 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae.
[91] Jailbreak. *Malwarebytes.* 2023. *https://www.malwarebytes.com/glossary/jailbreak*
[92] Unauthorized modification of iOS, Apple, 2023. https://support.apple.com/guide/iphone/unauthorized-modification-of-ios-iph9385bb26a/ios#:~:text=Jailbreaking%20your%20device%20eliminates%20security,Instability.
[93] Bill Marczak and John Scott-Railton, "The Million Dollar Dissident".

commercial spyware, so far as forensic analysts can tell; the first time was in 2011 with FinSpy, created by German firm FinFisher, followed by Italian firm Hacking Team's Remote Control System in 2012. Both firms became the subject of public controversy. FinFisher filed for bankruptcy following the start of a criminal investigation in the spring of 2022, for selling its spyware to Turkey without an export license[94]. Hacking Team was hacked in 2015, and a slew of the firm's internal documents and correspondence were leaked to the public, which led to the revocation of their Italian export license in 2016. Three years later, Hacking team was acquired by Paolo Lezzi and rebranded as Memento Labs [95].

In this 2016 case, Mansoor received strange text messages which contained links accompanied by baiting messages that "promised "new secrets" about detainees tortured in UAE prisons"[96]. Instead of clicking on the links, Mansoor forwarded the messages to Citizen Lab, and a team led by Senior Researcher, John Scott-Railton, downloaded the messages to a stock factory-reset iPhone to see if the links would download spyware to the phone. The links were active, and Citizen Lab for the first time was in possession of Pegasus spyware. To Citizen Lab's knowledge, this was the first time that one of NSO's products was undergoing a thorough technical analysis[97].

How Pegasus Works

In order to understand how Pegasus and Hungary thwarted regulation geared towards architecture, some technical details about spyware, and Pegasus in particular, need further

---

[94] ECCHR, "Surveillance software "made in Germany" for Turkish authorities?" *European Center for Constitutional and Human Rights,* 2023, https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/.
[95] Patrick Howell O'Neill, "The fall and rise of a spyware empire", *MIT Technology Review,* November 29, 2019, https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/#:~:text=Memento%20Labs%20was%20formed%20in,its%20products%20to%20potential%20customers.&text=That%20acquisition%20pulled%20together%20the,and%20development%20team%20from%20InTheCyber.
[96] Ibid.
[97] Ibid.

elucidation. Spyware cannot dismantle privacy on an iPhone through a single exploit if one is seeking to gain as much access to a phone as Pegasus does. Coders need to pull off an interconnected chain of events,, an 'exploit chain', in order to bypasses multiple layers of the phone's operating system to get to the 'kernel', which is "the set of programs in an operating system that implement the most primitive of that system's functions…typical kernels contain programs for five classes of functions… process management, memory management, interprocess communication, file and device management, and security."[98]All of that is a technical way of saying that kernel access is the gateway which Pegasus must cross in order to deliver the payload – the code that executes surveillance functions. Citizen Lab named the particular exploit chain and payload discovered in the Mansoor case, 'Trident'.

Accessing the kernel is difficult, but that's not what sets NSO apart. Rather, it is NSO's ability to access the kernel *and* consistently find new exploits after the ones they have in use are discovered and patched. Everytime an exploit chain is patched, firms like NSO have to pour time and resources into finding an entirely new way to reach the kernel. Kernel access is necessary to be able to do processes like record audio without the device's owner knowing.

When Citizen Lab discovered that the spyware was indeed Pegasus, and what it was capable of, they notified Apple, who was able to 'patch' the bug which NSO had been utilizing. Citizen Lab released their findings the same day that Apple released the software update which eliminated Trident's functionality for iOS. Less than a week later Apple also released security updates for the operating systems of Desktop Safari and Mac, as Trident was found to work on those systems as well[99].

---

[98] "KERNEL." In Encyclopedia of Computer Science, edited by Edwin D. Reilly, Anthony Ralston, and David Hemmendinger. Wiley, 2003. Accessed November 19, 2023. https://search.credoreference.com/articles/Qm9va0FydGljbGU6MTY2NTQ5OQ==?aid=100709.
[99]Bill Marczak and John Scott-Railton, " The Million Dollar Dissident".

Starting in 2019, Apple started offering up to 1 million dollars as a bounty for zero-day exploits capable of bypassing the most essential elements of iOS security[100]. The price tag reflects the level of skill needed to 'build' such a sophisticated exploit – to a point. One could argue that NSO level exploits should be priced higher; in an interview with Lex Fridman, Nicole Perlroth noted that if the WhatsApp and Apples of the world were to increase the price tag for NSO level zero-days, they could potentially disincentivize employees responsible for improving product security. High bounties risk becoming too high if they are so lucrative that highly skilled programmers choose to join the offense rather than the defense.[101]

Citizen Lab once again encountered 'something new' from NSO Group in 2021, an 'iMessage-based zero exploit', which Citizen Lab dubbed FORCEDENTRY. The Project Zero Team at Google, which received a sample of this iteration of Pegasus from Citizen Lab, said, "Based on our research and findings, we assess this to be one of the most technically sophisticated exploits we've ever seen, further demonstrating that the capabilities NSO provides rival those previously thought to be accessible to only a handful of nation states."[102]

Pegasus helps its clients overcome the architectural constraint of encryption, or the walls that otherwise stand in the way of their clients from being able to intercept and read targets' messages.[103] In simplest terms, end-to-end encryption services like WhatsApp scramble the code of the messages that users send on its platform, such that the contents of those messages cannot

---

[100] Thomas Brewster. "Apple Confirms $1 Million For Anyone Who Can Hack an iPhone". *Forbes*. August 8th, 2019. https://www.forbes.com/sites/thomasbrewster/2019/08/08/apple-confirms-1-million-reward-for-hackers-who-find-serious-iphone-vulnerabilities/?sh=503d3f1e3948.

[101] Nicole Perlroth interviewed by Lex Fridman, Nicole Perlroth: Cybersecurity and the Weapons of Cyberwar, February 20, 2022. https://www.youtube.com/watch?v=hy2G3PhGm-g.

[102] Google Project Zero, "A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution", Google Project Zero, December 15, 2021, https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html.

[103] Papademetriou, 102.

be descrambled or revealed unless the receiver has a 'key'[104]. Encryption prevents those who 'don't hold the key' from seeing your messages — law enforcement included. Instead of using spyware (as far as we know) the U.S. government has used other ways to try to circumvent encryption's constraint on intelligence gathering. The US' National Security Agency (NSA), became the subject of public outrage following the Snowden revelations in 2013, when the NSA's PRISM program (Planning Tool for Resource Integration, Synchonization, and Management) came to light. PRISM is not as efficient as spyware for real-time surveillance of a target and requires sourcing information from a variety of platforms (Gmail, Facebook, Outlook, etc.) and negotiating with those platforms in order to get access .[105] PRISM tracks international communications and the FISA court is responsible for providing warrants for the program's operations. Americans are not supposed to be singled out as sole targets, but the government has admitted that the private communications of American citizens do get caught up in data collection for the PRISM program. PRISM does not allow for seamless, in real-time data collection on an individual as easily as Pegasus does, instead it stores data in a searchable database for intelligence officials.[106] As stated in a 2013 article from The Verge, "NSA programs collect two kinds of data: metadata and content. Metadata is the sensitive byproduct of communications, such as phone records that reveal the participants, times and durations of calls; the communications collected by PRISM include the contents of emails, chats, VoIP calls, cloud-stored files, and more"[107].

---

[104]Google Cloud, " What is encryption?" Google, 2023, https://cloud.google.com/learn/what-is-encryption#:~:text=on%20every%20day.-,How%20encryption%20works,also%20created%20by%20an%20algorithm.
[105] T.C. Sottek and Janus Kopfstein, "Everything You Need to Know About PRISM", *The Verge,* July 17, 2013, https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.
[106] Patrick Toomey, "The NSA Continues to Violate Americans' Internet Privacy Rights", *ACLU*, August 22, 2018, https://www.aclu.org/news/national-security/nsa-continues-violate-americans-internet-privacy.
[107] Ibid.

Unlike PRISM, the encryption problem is eliminated instantaneosly with Pegasus, because everything on the phone can be seen by the client *after* messages have been decrypted, in real time. Content does not need to be sourced from different providers, and in the case of Hungary, the architecture of Pegasus works well with the legal system, which only needs the Minister of Justice to authorize permission for secret surveillance. Following that, there is no red tape on what can be surveilled, which makes Pegasus an architecturally efficient fit for illegal surveillance.

In the cases of Andras Szabo, Szabolcs Panyi, Brigitta Csikacz, and Daniel Nemeth, analysis performed on their devices by Amnesty International (then peer reviewed by Citizen Lab) concluded that all three of their phones were infected with Pegasus through an iMessage exploit chain, and that the code containing Pegasus came from a single iMessage account[108]. This information allows one to reasonably conclude that their phones were infected by a single operator. However, Citizen Lab was unable to prove the identity of that operator. A report published by Citizen Lab in 2018 identified 36 different Pegasus operators, which is another way of saying internet servers responsible for deploying Pegasus infections[109]. Citizen Lab deduced from the geographic features of domain names (URLs), that two of those operators may have been set up to cause Pegasus infections in Hungary. [110] However those conclusions are built on inferences which would not necessarily help a victim's case in a court of law.

Despite the fact that Citizen Lab and other organizations like it have been able to analyze Pegasus code from infected devices, other architectural features of the surveillance operations in

[108] Szabolcs Panyi and Andras Petho. "Hungarian journalist reporting on corruption surveilled with Pegasus for months". *Direkt36.* August 2, 2021. https://www.direkt36.hu/en/honapokon-at-megfigyeltek-pegasusszal-egy-korrupcios-ugyeken-is-dolgozo-magyar-bunugyi-ujsagirot/.
[109] Bill Marczack et al, "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries," Citizen Lab, September 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.
[110] Ibid.

which Pegasus is used remains a mystery. Former NSO CEO Shalev Hulio, once stated that when the company investigates allegations of abuse, they can compel logs from their clients which reveal who their targets are[111]. A different time he said, "NSO does not operate the systems that it sells to vetted government customers and does not have access to the data of its customers' targets yet [its customers] are obligated to provide us with such information under investigations."[112] If NSO does not have access to clients' operational data involving Pegasus, then how can they possibly verify that target lists provided by clients are accurate? NSO cannot claim that they are accurate without being able to verify the lists themselves, which would imply that they are able to overcome any architectural hurdles which would stand in the way of

Norms

The international community has failed to establish a cohesive set of norms that would protect journalists from spyware surveillance. The United Nations has tried to protect privacy rights to some extent – Article 17 of the UN's International Covenant on Civil and Political Rights, adopted on December 16, 1966 states that:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks. [113]

In order to improve the incorporation of the technological side of surveillance , the UN adopted General Comment. No 16 on Article 17 in 1988 to include "Surveillance, whether electronic or otherwise, interceptions of telephonic, telegraphic and other forms of communication, wire-tapping and recording of conversations should be prohibited" and that

[111] Patrick Howell O'Neill, "The man who built a spyware empire says it's time to come out of the shadows", August 19, 2020, *MIT Technology Review,* https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/.
[112] "Response from NSO and governments", *The Guardian,* July 20, 2023. https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments.
[113] Office of the High Commissioner United Nations Human, "International Covenant on Civil and Political Rights", Rights, The United Nations, 2023, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

"Even with regard to interferences that conform to the Covenant, relevant legislation must specify in detail the precise circumstances in which such interferences may be permitted".[114] As Papademetriou pointed out in his article, the UN has not updated Article 17 to include the myriad of technological advancements since 1988, and continues to maintain very general definitions of what constitutes "arbitrary" or "unlawful" interference. Thus, states and firms have been able to exploit such vagueness to exploit such vagueness to excuse privacy infringing behavior in ways that their citizens would have reasonably expected protection from.[115]

In the case of Hungary, the country benefited from the fact that Israel did not require EU member states to file individual human rights assessments in order to apply for an export license for surveillance products like Pegasus – apparently EU membership was considered proof enough that a country like Hungary would not misuse Pegasus.[116] After confirming that forensic examination found Pegasus on the phones of three Hungarians (presumably the journalists named in this paper), Hungarian Justice Minister Judit Varga said at a press conference that, "Hungary is a state governed by the rule of law, and like any decent state, in the 21st century it has the technical means to carry out its national security tasks…It would be a serious problem if we did not have these tools, but they are used in a lawful manner".[117] Technically speaking, what Varga said was true. As this paper recounted in the earlier section on laws, Hungary's secret surveillance laws technically do allow for Pegasus to be used for a wide range of purposes falling under the umbrella of national security – despite international pressure (like the European Court of Human Rights) to change *how* those laws are applied. NSO's own Human Rights Policy,

[114] Office of the High Commissioner, CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. United Nations. April 8, 1988. https://www.refworld.org/pdfid/453883f922.pdf.
[115] Papademtriou, "Disrupting Digital Authoritarians".
[116] Feldstein and Kot, 8
[117] Michael Bernbaum, Andras Petho, and Jean-Baptiste Chastand. "In Orban's Hungary, spyware was used to monitor journalists and others who might challenge the government". *The Washington Post.* July 19, 2021. https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/.

which the firm published in 2019, mirrors the language used by Varda, "Our goal is to ensure that our customers use our products only in accordance with their governing law and for necessary contracted purposes."[118] So long as international institutions like the UN fail to provide further specification on what is and is not acceptable privacy invasion under surveillance law, one should expect justifications like the ones provided by Hungary and NSO when countries and firms are caught misusing spyware.

As Lubin's article pointed out, the United States has tried to bring about a multilateral shift in norms through its Summit for Democracy initiatives. Forty-five participating states were signatories of the Guiding Principles on Government Use of Surveillance Technologies as of March 2023, when the Summit met for the second time. The five page, non-binding document is "intended to prevent the misuse of surveillance technologies by governments to enable human rights abuses in three main areas: the use of Internet controls; Pairing video surveillance with artificial-intelligence driven tools; and the use of big analytic data tools".[119] However the document does not describe how adherence to the Principles will be assessed, nor does it specify how states who choose to uphold the norms will stand to benefit, besides doing 'the right thing', a shortcoming which is also acknowledged by Lubin[120]. How signatories will benefit politically, or in terms of national security, is a question worth asking. While some countries guilty of spyware misuse, such as Spain, Greece and Poland have signed the pledge, Hungary has not. Because the pledge is non-binding, there is no mechanism for enforcing compliance – other

[118] NSO Group, Human Rights Policy, September 2019, https://www.nsogroup.com/wp-content/uploads/2019/09/NSO-Human-Rights-Policy_September19.pdf.
[119] U.S. Department of State,"Guiding Principles on Government Use of Surveillance Technologies", March 30, 2023, https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/.
[120] Lubin, 16.

incentives must presumably be expected to take the place of clear penalties, if the pledge is expected to work.[121]

Discussion

The findings from Lessig's Four Modalities as applied to the case of Pegasus in Hungary case will now be used as points of reflection to evaluate some of the proposed solutions for combating spyware misuse covered in the literature review. The viability of those regulatory propositions depend on whether there are countries which sincerely want to make changes that would make it more difficult for governments to use spyware for illegal purposes. That sincerity should not be taken for granted – for actual change to take effect, a government's drive to do so must go beyond the aspirations of a single leader or administration, whose time in office is limited. Applying Lessig's Four Constraints to analyze Hungary's use of spyware brought to light information that may be useful to scholars who are interested in finding solutions to combat spyware.

In terms of laws, the European Court of Human Rights ruled in 2016 that Hungary's surveillance law violated Article 8 of the European Convention of Human Rights. However, it was not the broad language describing national interests which violated Article 8. The combined reasons which the Court ruled caused the violation was 7/E(3)'s lack of judicial oversight, the fact that motions sent to the Minister of Justice did not need to state with specificity why targets were chosen for surveillance, and that no mechanism existed to notify targets that they had been surveilled once that surveillance had ended. This ruling may weaken the strength of Lubin's CSAS framework, which Lubin developed in accordance with the European Court of Human

[121] Current signatories include Albania, Argentina, Australia, Austria, Canada, Chile, Bulgaria, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Ecuador, Estonia, Finland, France, Georgia, Germany, Ghana, Greece, Iceland, Ireland, Italy, Japan, Kenya, Kosovo, Latvia, Lithuania, Luxembourg, Maldives, Malta, Mexico, Moldova, Mongolia, Netherlands, New Zealand, North Macedonia, Norway, Poland, Slovakia, Slovenia, Spain, Sweden, Switzerland, Tunisia, the United Kingdom, Ukraine, and the United States.

Rights' case law on technology and human rights, citing *Szabo and Vissy v. Hungary (2016)*, *Ivaschenko v. Russia (2018)* , *Big Brother Watch v. United Kingdom (2021)* as supporting evidence.

Under CSAS, governments would have to follow a human rights framework when deciding how to use spyware, and spyware firms would have to apply the principles in how they develop and market spyware, as well as how they manage client relationships. The governing principles would be:

1. Principle of Legality
2. Principle of Necessity
3. Principle of Proportionality
4. Principle of Adequate Safeguards
5. Principle of Access to Remedy and Transparency[122]

However, Lubin's idea that these principles, and by extension, the EUCtHR's case law relevant to spyware, which Lubin cited, would prevent spyware from being used on journalists or dissidents for political motivations, is not necessarily true, mostly because the Court has tried to avoid diving into the particulars of what differentiates a good reason to select someone for targeting from a bad one. For instance, in Ivaschenko v. Russia, the EUCtHR ruled that it was illegal for a Russian customs official to download the contents of a Russian journalist's laptop because they did so without a warrant and without demonstration of reasonable suspicion. The search and seizure was not "in accordance with the law". Had a warrant been issued based on 'reasonable suspicion', the official's actions may have been considered permissible. For instance, the fact that the journalist was returning from a 'disputed' area, Azbahkia, was not considered sufficient reasoning for the search according to the EUCtHR. However, what if Ivaschenko had been in contact with someone Russia considered a threat to national security? That would be a

[122] Lubin, 31.

more difficult question for the EUCtHR to answer, but the kind of answer that is needed in order for the Court's principles to be useful in the spyware arena, particularly where the press are concerned.[123]

The case of Big Brother Watch and Others v. the United Kingdom involved bulk interception of data, not targeted surveillance.[124] Like Ivaschenko v. Russia, the case does not provide specific insight into what kind of behavior would warrant becoming the target of spyware surveillance. While the EUCtHR's principles are well established within the international community's understanding of human rights, they have provided no definitive answers on the line between a person who the government doesn't like, and a person whose behavior is so threatening to national interests that a surveillance authority has no other option than to use spyware to surveil them. Governments are not the only ones slow or unwilling to make these distinctions, international human rights courts are as well, and may not be as helpful as one would hope in determining new norms for spyware use.

Analyzing the market forces of the spyware industry showed that spyware is not particularly expensive compared to other means of surveillance, and that the cost of acquiring and maintaining the Pegasus system has ample wiggle room to adjust to the practical needs and budget of different countries and their respective agencies. The spyware marketplace enables, rather than disincentivizes, spyware use, especially when countries appear to feel that their return on investment will be worth it. An important question to consider is how the cost of spyware surveillance would change if the commercial spyware industry suddenly disappeared, and governments could only rely on their in-house capabilities. While that question was outside the

[123] The European Court of Human Rights, *Legal Summary, Ivaschenko v. Russia,* Council of Europe, February 2018, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-11847%22]}.
[124] The European Court of Human Rights, *Legal Summary, Big Brother Watch and Others v. the United Kingdom,* Council of Europe, May 2021, https://hudoc.echr.coe.int/eng?i=002-13278.

scope of this study, if that were to happen it wouldn't necessarily mean that spyware misuse would go away. Firms like NSO offer countries access to expertise that they might not be able to cultivate on their own. However, countries with higher capacity for developing and retaining talent for surveillance technology purposes may use this capability to offer their services as a way to influence their relations with other countries. For example, the IDF's Unit 8200 gives young Israelis the requisite skills for conducting offensive cyber operations, some of whom take these skills to spyware firms like NSO.[125] Israel is much better positioned to deal with increased spyware regulation than countries like Hungary. Even if civil litigation were able to bankrupt the industry, illegal spyware operations wouldn't disappear, but the ability to conduct them would be further concentrated in the hands of a small group of countries. Therefore, scholars should not assume that increased regulation of the commercial spyware industry will necessarily translate into better state behavior. In addition it could push the availability of information on spyware operations even further into the shadows. Governments would no longer be exchanging information with commercial entities, leaving details of their surveillance operations less susceptible to instances of public discovery like The Pegasus Project's acquisition of NSO's 'potential targets list'.

The architectural features of spyware make it effective for both conducting illegal surveillance and avoiding legal responsibility for it afterwards. In the case of Hungary, various factors like the single iMessage account, the clustered timing of the infections during EU Article 7 proceedings, the kinds of journalists targeted, the presence of operators who were likely focused on Hungarian targets, as well as the government's own admission that it acquired Pegasus, points to the Hungarian government as the guilty party in the use of Pegasus on those

[125] Ronen Bergman and Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon", The New York Times Magazine, January 28, 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

four Hungarian journalists. However, it is still a slow and difficult process to be able to prove Hungary guilty, or NSO for that matter, in a court of law.

Papademetriou suggested that increasing access to forensic analysis may help victims bring standing against bad actors like Hungary. Generally speaking, it is difficult to prove that spyware definitively originates from a single firm, because code is not traceable in the way that things in the real world are, and anyone could technically copy the code of another firm's product. Back in 2018 a former NSO employee tried, and failed, to sell Pegasus on the black market for $50 million.[126] Had they succeeded, NSO's proprietary code would have fallen into the hands of someone else, and forensic analysts would have had a much harder time figuring out whether a Pegasus infection had originated from a client of NSO or some other firm. Lubin proposes watermarking software as a part of his CSAS framework in order to more definitively attribute the origins of spyware infections.[127] Lubin's intent behind watermarking is so that CSAS can track whether firms who join the agreement actually adhere to the framework's human rights guidelines, which requires that signatories not work with clients who don't pass CSAS's vetting process, or whose contracts must be terminated following an incident of misuse. That way, if an infection appears on the device of a target who is being illegally surveilled, CSAS knows which firm sold that particular spyware. There are many ways to watermark software, and watermarks are themselves susceptible to hacking.[128] What watermarking method Lubin chooses to use, and whether firms will have a choice in how they watermark their software, will matter.

---

[126] Joseph Cox, "NSO Group Employee Allegedly Stole Company's Powerful Spyware for Personal Profit", Vice, July 5, 2018, https://www.vice.com/en/article/9km99z/nso-group-employee-stole-code-sell-dark-web-50-million.
[127] Lubin, 34
[128] Dey, Ayan & Bhattacharya, Sukriti & Chaki, Nabendu. (2018). Software Watermarking: Progress and Challenges. INAE Letters. 4. 10.1007/s41403-018-0058-8. PAGE 7 https://www.researchgate.net/publication/328409630_Software_Watermarking_Progress_and_Challenges.

These considerations highlight the importance of accounting for architectural features in policy proposals, and that regulation predicated on architectural regulation may be difficult to enforce.

Lastly, it is difficult to ascertain the extent to which Hungary departed from norms by using spyware to illegally surveil journalists, since the right to privacy in the context of spyware is still a muddled concept. It is easy for states to call out others for spyware surveillance that is so clearly illegal and politically motivated, but condemnation seems to be where most of their energy goes. States feel that they have the right to enforce their own definitions of national interests and national security. The European Court of Human Rights reflects this prerogative in the "margin of appreciation concept", which the Court provided as explanation for why they did not find issue with the broad wording of "national interests", in Szabo and Vissy v. Hungary. What constitutes a legitimate national interest can depend on information that the government is reluctant to make public knowledge, even to other states. While one can debate the merits of surveilling a reporter who covers corruption in government (and of course some will say it's not a debate – they shouldn't), it's important to, once again, recognize that it is not always easy to define who merits targeted surveillance and who doesn't. Which is most likely why deliberation between governments – at least on a broad international level – addressing the specifics of acceptable use cases for spyware hasn't happened. Of course, not all government discussions are made public. But by managing to avoid it, countries protect themselves from critique. Instead, they tell each other, perhaps figuratively rather than literally, "I'll let you do what you need to do, so long as you let me do what I need to do". Therefore it seems plausible that the strongest explanation for why norms have not changed for the better is because states are interested in maintaining their prerogative to conduct national security as they see fit, rather than improving norms governing privacy rights.

Conclusion

Lessig's Four Modalities of Regulation was a useful framework for approaching and analyzing information pertaining to Hungary's use of Pegasus on journalists. From the outset it was already known that regulatory constraints have failed to stop illegal spyware surveillance from happening. However, analysis of those constraints through Hungary as a case study seemed to generate an overarching answer for why states haven't done more to prevent the use of spyware to surveil journalists. It is not just because effective regulation is difficult to formulate for spyware as a product, but because effective regulation in this context would be highly dependent on state's deploying large amounts of political capital to enforce it. States have shown little interest in making effective regulation, most likely because doing so would infringe on their ability to unilaterally, and expediently use spyware for purposes that will likely not be deemed acceptable on the public stage, and because other issues take priority.

Covering all four of Lessig's Modalities for this study required looking at how a government used spyware illegally from various conceptual perspectives; with each changing view came more questions and areas for further research. For instance, looking at the regulation of anything in an international context brings up differences in how nations approach law, much less something as complicated and ever-developing as spyware. A possible, ongoing project could be a comparative study between countries, looking at potential differences in the level of evidence needed for one to successfully assert causation against a spyware firm, or otherwise prove in a court of law that a firm's product was used for illegal surveillance purposes. Perhaps some state's judicial and legal landscape is better suited for these kinds of lawsuits than others. Another area of study that deserves more attention is the resiliency and capacity of commercial firms to meet client needs when facing financial limitations. For instance, how much money does

a firm generally need from investors in order to create a product that uses the kind of exploit that Apple is willing to pay $1 million for? If a firm lacks funds, how low can its financial standing be while still keeping the company operational and retaining highly skilled developers. This question is intended to challenge the idea that a company needs to be like NSO, once valued at $1 billion, in order to cause considerable harm to journalists and others.

By focusing on the use of spyware in a single country, this paper was able to observe how state use of commercial spyware challenges regulations in the areas of law, markets, architecture, and norms. However, analysis of those findings, particularly in reference to current regulatory proposals, provided insight on how the nature of spyware and states' current attitudes towards it, will continue to pose a threat to the privacy of journalists, and others integral to the functioning of democracy, on a global scale.

Works Cited

Administrative Office of the U.S. Courts, *Wiretap Report 2021*, United States Courts, December 31, 2021, https://www.uscourts.gov/statistics-reports/wiretap-report-2021.

"Massive data leak reveals Israeli NSO spyware used to target activists, journalists, and political leaders globally". Amnesty International. July 19, 2021. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.

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

Birnbaum et al. "In Orban's Hungary, spyware was used to monitor journalists and others who might challenge the government". *The Washington Post.* July 19, 2021. https://www.washingtonpost.com/world/2021/07/18/hungary-orban-spyware/.

Brewster, Thomas. "A Multimillionaire Surveillance Dealer Steps Out of The Shadows…And His $9 Million WhatsApp Hacking Van". *Forbes*. August 5, 2019. https://www.forbes.com/sites/thomasbrewster/2019/08/05/a-multimillionaire-surveillance-dealer-steps-out-of-the-shadows-and-his-9-million-whatsapp-hacking-van/?sh=48d9948331b7.

Brewster, Thomas. "Apple Confirms $1 Million For Anyone Who Can Hack an iPhone". *Forbes*. August 8th, 2019. https://www.forbes.com/sites/thomasbrewster/2019/08/08/apple-confirms-1-million-reward-for-hackers-who-find-serious-iphone-vulnerabilities/?sh=503d3f1e3948.

Case of Szabó and Vissy v. Hungary, 37138/14. HUDOC. EUCtHR 4th Section. January 12, 2016. https://hudoc.echr.coe.int/eng?i=001-160020.

Citizen Lab. "NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases". University of Toronto. October 29, 2019. https://citizenlab.ca/2019/10/nso-q-cyber-technologies-100-new-abuse-cases/.

Cox, Joseph. "NSO Group Employee Allegedly Stole Company's Powerful Spyware for Personal Profit", Vice, July 5, 2018, https://www.vice.com/en/article/9km99z/nso-group-employee-stole-code-sell-dark-web-50-million.

Dey, Ayan & Bhattacharya, Sukriti & Chaki, Nabendu. (2018). Software Watermarking: Progress and Challenges. INAE Letters. 4. 10.1007/s41403-018-0058-8. PAGE 7 https://www.researchgate.net/publication/328409630_Software_Watermarking_Progress_and_Challenges.

Dwoskin, Elisabeth and Shira Rubin. "NSO Group vows to investigate spyware abuse following Pegasus investigation". *The Washington Post*. July 20, 2021. https://www.washingtonpost.com/technology/2021/07/18/reactions-pegasus-project-nso/.

Dwoskin, Elisabeth and Shira Rubin. "'Somebody has to do the dirty work': NSO founders defend the spyware they built". *The Washington Post*. July 21, 2021. https://www.washingtonpost.com/world/2021/07/21/shalev-hulio-nso-surveillance/.

ECCHR, “Surveillance software “made in Germany” for Turkish authorities?” *European Center for Constitutional and Human Rights,* 2023, https://www.ecchr.eu/en/case/surveillance-software-germany-turkey-finfisher/.

EU Commission. “Rule of law conditionality regulation”. 2022. https://commission.europa.eu/strategy-and-policy/eu-budget/protection-eu-budget/rule-law-conditionality-regulation_en.

The European Court of Human Rights, *Legal Summary, Ivaschenko v. Russia,* Council of Europe, February 2018, https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22002-11847%22]}.
The European Court of Human Rights, *Legal Summary, Big Brother Watch and Others v. the United Kingdom,* Council of Europe, May 2021, https://hudoc.echr.coe.int/eng?i=002-13278.

European Parliament. “European Parliament resolution of 10 June 2015 on the situation in Hungary” (2015/2700(RSP)) June 10 2015. https://www.europarl.europa.eu/doceo/document/TA-8-2015-0227_EN.html.

European Parliament “European Parliament resolution of 16 December 2015 on the situation in Hungary” (2015/2935(RSP)) December 16, 2015 https://www.europarl.europa.eu/doceo/document/TA-8-2015-0461_EN.html.

Europen Parliament. “ European Parliament resolution of 17 May 2017 on the situation in Hungary” (2017/2656(RSP)) May 17, 2017. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0216_EN.html.

European Parliament. “European Parliament resolution of 12 September 2018” (2017/2131(INL)) September 12, 2018. https://www.europarl.europa.eu/doceo/document/TA-8-2018-0340_EN.html#def_1_2.

European Parliament. *Investigation of the use of Pegasus and equivalent spyware (Recommendation).* June 15, 2023. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.pdf.

Eotvos Karoly Intezet, “Introduction”, 2015, https://www.ekint.org/en/about.

European Court of Human Rights, *Guide on Article 8 - Right to respect for private and family life, home and correspondence*.Strasbourg: August 8, 2022. https://www.echr.coe.int/documents/d/echr/guide_art_8_eng.

“Szabolcs Panyi”, *Forbidden Stories*, https://forbiddenstories.org/journaliste/szabolcs-panyi/.

Feldstein, Steven and Brian Kot, “Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses”. Carnegie Endowment for International Peace. March 15, 2023. https://carnegieendowment.org/files/Feldstein_Global_Spyware.pdf.

Gall, Lydia. “Hungarian Government Stoops to New Low with Hate Campaign”. *Human Rights Watch.* July 12, 2017. https://www.hrw.org/news/2017/07/12/hungarian-government-stoops-new-low-hate-campaign.

Google Cloud, “ What is encryption?” Google, 2023, https://cloud.google.com/learn/what-is-encryption#:~:text=on%20every%20day.-,How%20encryption%20works,also%20created%20by%20an%20algorithm.

Google Project Zero. “A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution”. Google. December 15, 2021.
https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

The Greens/European Free Alliance. “Rule of Law: Commission Triggering of Conditionality Mechanism Against Hungary Long Overdue.” April 27, 2022.
https://www.greens-efa.eu/en/article/press/rule-of-law-commission-triggering-of-conditionality-mechanism-against-hungarian-government-long-overdue.

Hervey, Ginger and Emmet Livingstone. “What is Article 7?”. *Politico.* January 13, 2016.
https://www.politico.eu/article/hungary-eu-news-article-7-vote-poland-rule-of-law/.

Howell O’Neill, Patrick. “The fall and rise of a spyware empire”, *MIT Technology Review,* November 29, 2019.
https://www.technologyreview.com/2019/11/29/131803/the-fall-and-rise-of-a-spyware-empire/#:~:text=Memento%20Labs%20was%20formed%20in,its%20products%20to%20potential%20customers.&text=That%20acquisition%20pulled%20together%20the,and%20development%20team%20from%20InTheCyber.

Howell O’Neill, Patrick. “The man who built a spyware empire says it’s time to come out of the shadows”. August 19, 2020. *MIT Technology Review.*
https://www.technologyreview.com/2020/08/19/1007337/shalev-hulio-nso-group-spyware-interview/

Human Rights Watch. *Wrong Direction on Rights: Assessing the Impact of Hungary’s New Constitution and Laws.* HRW. May 16, 2013.
https://www.hrw.org/report/2013/05/16/wrong-direction-rights/assessing-impact-hungarys-new-constitution-and-laws.

Hungary. *The World Bank,* 2023, https://data.worldbank.org/country/hungary.

“Hungary’s Orbán government invests in spying technology for use abroad”. *Hungarian Free Press.* July 9, 2015.
https://hungarianfreepress.com/2015/07/09/hungarys-orban-government-invests-in-spying-technology-for-use-abroad/.

IBM“What is a zero-day exploit?”. Accessed December 13th, 2023.
https://www.ibm.com/topics/zero-day.

Kaster, Sean D. and Prescott C. Ensign. “Privatized espionage: NSO Group Technologies and its Pegasus spyware”, *Thunderbird International Business Review*. December 1, 2022.
https://doi.org/10.1002/tie.22321

Katibah, Leila. “The Politics of Pegasus Spyware: Examining the Impact of Surveillance on Journalism.” Undergraduate Thesis, University of California, Santa Barbara, 2023.
https://escholarship.org/uc/item/02k620g6.

Kirchgaessner, Stephanie. “Phones of journalist who tracked Viktor Orban’s childhood friend infected with spyware”, *The Guardian,* September 21, 2011,

https://www.theguardian.com/news/2021/sep/21/hungary-journalist-daniel-nemeth-phones-infected-with-nso-pegasus-spyware.

"KERNEL." In Encyclopedia of Computer Science, edited by Edwin D. Reilly, Anthony Ralston, and David Hemmendinger. Wiley, 2003. Accessed November 19, 2023. https://search.credoreference.com/articles/Qm9va0FydGljbGU6MTY2NTQ5OQ==?aid=100709.

Koenen, Krisztina . Hungary and the EU: A deepening divide. *GIS Reports*. May 17, 2023. https://www.gisreportsonline.com/r/hungary-eu-divide/.

Lessig, Lawrence. *Code 2.0.* New York: Basic Books, 2006.

Levitt, Spencer. "The European Parliament's PEGA Committee: A Regional Effort to Constrain Spyware Technology", UCI Law International Justice Clinic. January 25, 2023. https://ijclinic.law.uci.edu/2023/01/25/the-european-parliaments-pega-committee-a-regional-effort-to-constrain-spyware-technology/.

Libeiro, Jorge and Sandor Zsiros." Hungary is no longer a full democracy but an 'electoral autocracy', MEPS declare in new report." *euronews.* Updated September 16, 2022. https://www.euronews.com/my-europe/2022/09/15/hungary-is-no-longer-a-full-democracy-but-an-electoral-autocracy-meps-declare-in-new-repor.

Lubin, Asaf. *Regulating Commercial Spyware*. Washington, DC: The Lawfare Institute, August, 2023. https://www.lawfaremedia.org/article/regulating-commercial-spyware.

Maas, Peter. "U.S. Interests Try to Counter Hungarian Rightist". *The Washington Post.* October 20, 1992. https://www.washingtonpost.com/archive/politics/1992/10/20/us-interests-try-to-counter-hungarian-rightist/ed26f474-a87f-4770-b27b-eff89aadba72/.

Marczak, Bill and John Scott-Railton. "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender" Citizen Lab. August 24, 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae.

Marczack, Bill et al. "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries". Citizen Lab. September 18, 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

"Margin of Appreciation", Open Society Justice Initiative, April 2012", https://www.justiceinitiative.org/uploads/918a3997-3d40-4936-884b-bf8562b9512b/echr-reform-margin-of-appreciation.pd

"Massive data leak reveals Israeli NSO spyware used to target activists, journalists, and political leaders globally". Amnesty International. July 19, 2021. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/.

MEE Staff, " Pegasus: MBS called Netanyahu to renew Saudi Arabia's NSO license, report says. January 28, 2022, https://www.middleeasteye.net/news/pegasus-saudi-arabia-mbs-called-netanyahu-renew-nso-spyware-license-report-says.

"Mexico says officials spent $61 million on Pegasus spyware". Mexico City AP. July 18, 2021. https://www.pbs.org/newshour/world/mexico-says-officials-spent-61-million-on-pegasus-spyware.

Nicole Perlroth interviewed by Lex Fridman, Nicole Perlroth: Cybersecurity and the Weapons of Cyberwar, February 20, 2022. https://www.youtube.com/watch?v=hy2G3PhGm-g.

Nobahar, Gretchen. "Spyware" in *Privacy Rights in the Digital Age,* edited by Jane E. Kirtley and Michael Shally-Jensen. Grey House Publishing, 2019, accessed September 25, 2023, https://search.credoreference.com/articles/Qm9va0FydGljbGU6NDc5NTYyNg==.

NSO Group. Human Rights Policy. September 2019. https://www.nsogroup.com/wp-content/uploads/2019/09/NSO-Human-Rights-Policy_September19.pdf.

Office of the High Commissioner, UN. "International Covenant on Civil and Political Rights". The United Nations. 2023. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

Office of the High Commissioner, CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. United Nations. April 8, 1988. https://www.refworld.org/pdfid/453883f922.pdf.

Panyi, Szabolcs. "The inside story of how Pegasus was brought to Hungary". *Direkt36*. September 28, 2022. https://www.direkt36.hu/en/feltarulnak-a-pegasus-kemszoftver-beszerzesenek-rejtelyei/.

Panyi, Szabolcs. "Boosting of Spying Capabilities Stokes Fear Hungary Is Building a Surveillance State", *Balkan Insight*. October, 23, 2022.
Szabolcs Panyi and Andras Petho. "Hungarian journalists and critics of Orban were targeted with Pegasus, a powerful Israeli cyberweapon". *Direkt36.* July 19, 2021. https://www.direkt36.hu/en/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele/

Panyi, Szabolcs and Andras Petho, "Hungarian journalist reporting on corruption surveilled with Pegasus for months", *Direkt36*, August 2, 2021. https://www.direkt36.hu/en/honapokon-at-megfigyeltek-pegasusszal-egy-korrupcios-ugyeken-is-dolgozo-magyar-bunugyi-ujsagirot/.

Papademetriou, George T. "Disrupting Digital Authoritarians: Regulating the Human Rights Abuses of the Private Surveillance Software Industry." *Harvard Human Rights Journal.* 36, no. 2 (Spring 2023). https://journals.law.harvard.edu/hrj/wp-content/uploads/sites/83/2023/06/HLH105_crop.pdf.

PEGA Committee. *Mission Report: following the mission to Hungary – 20 and 21 February 2023.* Committee of Inquiry to investigate the use of Pegasus and equivalent surveillance spyware. April 20, 2023. https://www.europarl.europa.eu/doceo/document/PEGA-CR-746829_EN.pdf

Perlroth, Nicole. "How Spy Tech Firms Let Governments See Everything on a Smartphone". *New York Times*, September 2, 2016. https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html.

Priest, Dana. “A UAE agency put Pegasus spyware on phone of Jamal Khashoggi’s wife months before his murder, new forensics show”. *The Washington Post.* December 21, 2021. https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/.

“Response from NSO and governments”. *The Guardian.* July 20, 2023. https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments.

Schwarcz, Andras. Rule of law-related ‘super milestones’ in the recovery and resilience plans of Hungary and Poland. *European Parliament, Policy Department for Budgetary Affairs*. January 2023. https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/741581/IPOL_BRI(2023)741581_EN.pdf

Sottek, T.C. and Janus Kopfstein. “Everything You Need to Know About PRISM”. *The Verge.* July 17, 2013. https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet.

Spencer Levitt, “The European Parliament’s PEGA Committee: A Regional Effort to Constrain Spyware Technology”. UCI Law International Justice Clinic. January 25, 2023. https://ijclinic.law.uci.edu/2023/01/25/the-european-parliaments-pega-committee-a-regional-effort-to-constrain-spyware-technology/.

Spike, Justin. “Hungarian official: Government bought, used Pegasus spyware”. *AP News.* November 4, 2021.https://apnews.com/article/technology-europe-hungary-malware-spyware-ccacf6da9406d38f29f0472ba44800e0.

Stockholm International Peace Research Institute, “World military expenditure reaches new record high as European spending surges”. April 24, 2023. https://www.sipri.org/media/press-release/2023/world-military-expenditure-reaches-new-record-high-european-spending-surges.

“Szabolcs Panyi”, *Forbidden Stories*, https://forbiddenstories.org/journaliste/szabolcs-panyi/.

Szabo, Andras.“Andras Szabo, Hungarian Journalist”. Organized Crime and Corruption Project. July 18 2021. https://www.occrp.org/en/the-pegasus-project/andras-szabo-hungarian-journalist.

Timberg, Craig et. al. “On the list: Ten prime ministers, three presidents and a king”. *The Washington Post*. July 20, 2021. https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.

Toomey, Patrick, “The NSA Continues to Violate Americans’ Internet Privacy Rights”, *ACLU*, August 22, 2018. https://www.aclu.org/news/national-security/nsa-continues-violate-americans-internet-privacy.

UN General Assembly. *International Covenant on Civil and Political Rights*. December 16, 1966. *United Nations*. Treaty Series, vol. 999., https://www.refworld.org/docid/3ae6b3aa0.html.

U.S. Department of State. “Guiding Principles on Government Use of Surveillance Technologies”.March 30, 2023. https://www.state.gov/guiding-principles-on-government-use-of-surveillance-technologies/.

Walker, Shaun. “Dark Day for freedom’: Soros-affiliated university quits Hungary”. *The Guardian*. December 3, 2018.

https://www.theguardian.com/world/2018/dec/03/dark-day-freedom-george-soros-affiliated-central-european-university-quits-hungary.

WhatsApp Inc., and Facebook, Inc., v. NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. United States District Court Northern District of California. May 27, 2020. https://www.documentcloud.org/documents/6532395-WhatsApp-complaint.html.