The Pocket Assassin

Repression and intimidation are not - and never should be - the acceptable companions of reform. ~Jamal Khashoggi

Saudi Arabia has been frequently criticized for violating human rights. Freedom House a U.S.-based think tank that examines global repression gave Saudi Arabia a score of 8/100 (1/40 for political rights and 7/60 for civil liberties) and ranks the country as 'not free' in its 2023 annual country assessment report.[1] The country is known for mass executions, draconian prison sentences for women seeking political rights, and its complete lack of political and civil rights. The country is ruled by Crown Prince Mohammed bin Salman. The country institutes stringent religious and moral codes that constrain the rights of women. The Saudi ruling regime does not tolerate dissent.

Jamal Ahmad Khashoggi was born on October 13, 1958, in Medina Saudi Arabia. In the 1980s Khashoggi transitioned from managing bookstores to becoming a correspondent with the Saudi Gazette. In the mid 1980s while serving as a foreign correspondent he worked with Saudi Intelligence to monitor the Soviet War in Afghanistan. As Khashoggi's career progressed he increasingly expressed more liberal views that often brought him into direct conflict with the ruling Saudi regime. He began to push for Saudi Arabia to move towards secularism and towards constraining hardline Wahhabi Islamic traditions. By the early 2000s Khashoggi had gone into voluntary exile in the United Kingdom. In 2015 he launched Al-Arab a satellite news channel in Bahrain. The channel was only live for 11 hours before being closed by Bahraini officials. As his efforts to report were increasingly constrained by Saudi Arabia, he began engaging in political commentary on international news channels ranging from the BBC to Al Jazeera. In 2017 he relocated to the United States and began writing for the Washington Post. His commentary and criticism of the Saudi Regime continued. In particular, he became a vocal proponent of human rights and women's rights in Saudi Arabia. He also established the non-profit political organization Democracy for the Arab World Now (DAWN). His commentary, criticisms, and political action increasingly raised the ire of Crown Prince Mohammad Bin Salman. By early 2017 it was clear that Bin Salman and others felt threatened by Khashoggi and began issuing threats to his life.

Jamal Khashoggi was seemingly beyond the reach of the Saudi regime. He resided in the United States and took his personal security seriously. Yet, like most people he and his wife Hanan Elatr both had mobile telephones. On October 2, 2018, Khashoggi entered the Saudi consulate in Istanbul to obtain documents for his planned marriage and disappeared. Later intelligence

[1] "Freedom in the World 2023 - Saudi Arabia," *Freedom House*, 2023, https://freedomhouse.org/country/saudi-arabia/freedom-world/2023.

analysis would indicate that Khashoggi had been taken into custody and violently dismembered by members of a hit squad. As of 2022 26 Saudis nationals had been charged in connection with the gruesome killing by Turkish courts.[2]

A report written by the University of Toronto's Citizen Lab found that Khashoggi's wife and others in his inner circle were targeted with an advanced form of malware known as Pegasus prior to his assassination.[3] Further investigations would reveal that the malware was installed on his wife's mobile device when she was taken into custody by UAE officials in April 2018.[4] While Khashoggi's phones were not able to be examined, former NSA/CIA contractor and leaker Edward Snowden is quoted as saying that it is likely that the Saudi government used NSO's Pegasus spyware to track his movements.[5] The Khashoggi assassination is a horror story of mobile surveillance, but it is not a unique story.

Over the summer of 2021 a consortium of 17 media organizations investigated the development, sale, and use of the malware behind the Khashoggi murder. The organization traced the malware back to the Israeli cyber-arms company NSO Group. The consortium released a detailed report with a target list of more than 50,000 mobile phone numbers. The individuals behind these mobile numbers included opposition politicians, human rights activists, journalists, lawyers and political dissidents.[6] The NSO Group denied having its software used to hack into the mobile devices of these protected groups but Amnesty International released a damning report at the same time as the Pegasus project revealed the extent the spyware's reach indicating that the company was not being truthful in its rebuttals.[7] The released data indicates that thousands of individuals who have no ties to terrorism or criminal networks were the targets of state based surveillance using the Pegasus spyware developed and sold by the NSO group.

---

[2] Ayse Weiting and Suzan Fraser, "Turkish Court Moves Trial of 26 Saudis Suspected of Gruesome Khashoggi Killing to Saudi Arabia," *PBS*, April 22, 2022, https://www.pbs.org/newshour/world/turkish-court-moves-trial-of-26-saudis-suspected-of-gruesome-khashoggi-killing-to-saudi-arabia.

[3] Dana Priest, Souad Mekhennet, and Arthur Bouvart, "Jamal Khashoggi's Wife Targeted with Spyware before His Death," *The Washington Post*, July 18, 2021, https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/.

[4] 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/.

[5] Hagar Shezaf, "Snowden: Israeli Firm's Spyware Was Used to Track Khashoggi," *Haaretz*, November 7, 2018, https://www.haaretz.com/israel-news/2018-11-07/ty-article/.premium/israeli-spyware-was-used-to-track-saudi-journalist-khashoggi-edward-snowden-says/0000017f-e09f-df7c-a5ff-e2ffc1650000.

[6] Washington Post Staff, "Takeaways from the Pegasus Project," *The Washington Post*, August 2, 2021, https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

[7] "Forensic Methodology Report: How to Catch NSO Group's Pegasus" (London, UK: Amnesty International, July 18, 2021), https://www.amnesty.org/en/documents/doc10/4487/2021/en/.

Pegasus traces its development back to 2016 and has been steadily improved upon since that time. It is widely considered one of the world's most powerful cyber weapons.[8] Pegasus is powerful both for its ability to infect mobile devices stealthily and its ability to collect enormous volumes of data from across the target mobile device. According to tech journalist Kim Zetter Pegasus can be installed on target systems in one of three ways: physically, remotely via text message or email, or remotely through a 'silent' message pushed to the phone.[9] The phone of Jamal Khashoggi's wife appears to have been infected directly, while many of the phones identified in the Pegasus project appear to have been subjected to later more advanced versions of the malware and infected remotely. Among the data types that can be extracted from a targeted device are instant messages, photos and screenshots, microphone recordings, emails, SMS/MMS messages, location data from GPS or other satellite providers, network settings, device settings, browsing history, contact details, social network information, phone call information, calendar records, and all files contained within the mobile device. In essence once Pegasus is installed on a target system it has the potential to collect any and all information on that device. Moreover, Pegasus uses AES 128-bit encryption after compressing the data to send it back to its surveillance network and subsequently makes that data accessible to the surveilling customer who purchased the license. The software can determine whether the user is on WIFI or mobile networks. It can choose when to transmit data to prevent the target from knowing he or she is being surveilled because of higher data usage over mobile networks.[10]

The most nefarious attribute of the malware was its ability to harness a vulnerability in the way in which mobile phones render text and images in messaging applications. By sending the target an infected message the spyware can be installed silently in the background without the target having to click or do anything. Simply receiving a message is enough to initiate the infection.[11] Prior to the newer version of Pegasus including what are aptly called "zero-click" hacks, the software could also be used by taking advantage of network protocols in mobile phones using stingrays (rogue mobile based stations) to hijack the phone into believing that it was connecting to an actual mobile network provider using what is known as an SS7 (Signaling System No. 7) attack. This type of attack has been used by law enforcement agencies and militaries to track criminals and terrorists. It has also been used to provide tactical information to militaries on the front lines of the 2014-2022 war in the Donbas of Ukraine.[12]

---

[8] Ronen Bergman and Mark Mazzetti, "The Battle for the World's Most Powerful Cyberweapon," *The New York Times*, January 28, 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.
[9] Kim Zetter, "Pegasus Spyware: How It Works and What It Collects," *Zero Day*, August 4, 2021, https://zetter.substack.com/p/pegasus-spyware-how-it-works-and?utm_source=%2Fsearch%2Fpegasus&utm_medium=reader2.
[10] Ibid.
[11] Ibid.
[12] Aaron Brantly, Nerea Cal, and Devlin Winkelstein, "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW" (West Point, NY: United States Army Cyber Institute, December 1, 2017), http://www.dtic.mil/dtic/tr/fulltext/u2/1046052.pdf.

Individuals who have been targeted by spyware are frequently unaware of their targeting until they discover their device's battery draining more rapidly than normal or their data usage over mobile networks increasingly out of proportion with their expected use. When an individual's device is successfully penetrated using Pegasus or similar spyware their private lives are no longer private. The device in their pocket, carried with them everywhere they go is now a broadcast beacon that relays data to a third party. Everything from intimate photos or texts to work on investigative reporting on corrupt governments, or even work with human and democracy rights activists becomes exploitable. Moreover, this is not a post-hoc review of data but rather a live stream of data that captures the target's real-time movements.

The assassination of Jamal Khashoggi was facilitated using modern spyware that turned a device that most individuals carry and use daily into a digital spy. Mobile phones have become the repositories of individual information ranging from photos and emails to financial information and individual locations both over time and in real time. The mobile phone has become a trusted extension of daily life, that puts the conveniences and information of the world at the tip of the finger. Yet these devices are also increasingly tools of oppression and repression by state and non-state actors. Unfortunately, the case of Jamal Khashoggi is not isolated. Pegasus and similar spyware programs have been used to harass and target individuals in dozens of countries. They have even been used by criminal organizations to track down and murder individuals by criminal organizations. If the problem of having state and nonstate groups using spyware wasn't a sufficiently large problem, there is ample evidence that spyware is also frequently a tool of domestic abuse.[13]

The Jamal Khashoggi case and the findings of the Pegasus Project and research on the increasing reach of spyware raises multiple questions that challenge how mobile phones should be perceived. Not every smartphone will be used as a tracking device for state assassination, yet it is increasingly apparent that the phone that follows you everywhere you go is not necessarily a private or secure device. The devices once heralded for their ability to connect and facilitate change are increasingly becoming devices of surveillance and repression.

Question 1:
What kinds of information do you store on your phone? Take a few minutes to write down some of the different kinds of data that are on your phone. Do you have location data? Do you have information about your financial accounts? Do you have medical or health data on your phone? Are all your personal and professional contacts listed in your phone? Do you store personal

[13] Charlotte Jee, "How 'Stalkerware' Apps Are Letting Abusive Partners Spy on Their Victims," *MIT Technology Review*, July 10, 2019, https://www.technologyreview.com/2019/07/10/134249/stalkerware-apps-are-letting-abusive-partners-spy-on-their-victims/.

photos and videos on your phone? What are the implications of having all this data about you and others you care about on a device that goes everywhere you do?

Question 2:
The assassination of Jamal Khashoggi was not an isolated incident. There have been examples of multiple governments and criminal organizations leveraging similar software to target other individuals for various reasons. In Mexico cartels and the Mexican army have been implicated in using spyware against journalists.[14] The government of El Salvador has used Pegasus to surveil more than 35 journalists and human rights defenders.[15] Presently, there is little regulation on the development and sale of spyware. A subset of spyware called stalkerware has even less regulation. Should companies that develop and sell spyware be regulated? If so, what regulations should be placed on the sale of spyware?

Question 3
Spyware often takes advantage of vulnerabilities within mobile device software ecosystems. The development of mobile phone software is a complicated and iterative process. Every year new versions of software are released, and new vulnerabilities are found within that software that expose users to potential exploitation from malware such as spyware. Some types of vulnerabilities exploit the fundamental functioning of devices. Attacks against the signal acquisition systems of devices or against the rendering of text or images are very difficult to combat. What is the responsibility of mobile phone manufacturers and software developers to ensure that their software and hardware adequately protect their users against malware attacks? What is the responsibility of software and hardware developers and manufacturers to ensure patches are issued in a timely manner to fix vulnerabilities within their software and hardware ecosystems? Do these same responsibilities extend to legacy devices that are no longer supported by major software releases?

Question 4
The use of spyware and other forms of malware to surveil individuals seemingly conflicts with the Universal Declaration of Human Rights. Yet, while there has been substantial advocacy by organizations such as Human Rights Watch, Amnesty International, the Electronic Frontier Foundation and others, little progress has been made to apply human rights norms to challenges arising through digital technologies. How might states use the exploitation and targeting of individuals via digital means to advance norms to protect individuals in digital and non-digital spaces? Do you think human rights norms should be applicable in digital spaces and on personal

[14] Stephanie Kirchgaessner, "Mexico: Reporters and Activists Hacked with NSO Spyware despite Assurances," *The Guardian*, October 4, 2022, https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked-pegasus.
[15] Sam Jones, "Pegasus Spyware Used in 'Jaw-Dropping' Phone Hacks on El Salvador Journalists," *The Guardian*, January 13, 2022, https://www.theguardian.com/news/2022/jan/13/pegasus-spyware-target-journalists-activists-el-salvador.

digital devices? If you were to construct norms for states to adhere to in digital spaces, what would they constitute? How might they be enforceable?

Question 5

Many organizations such as the EPIC (Electronic Privacy Information Center), EFF, Amnesty International, the Citizen Lab, the National Democratic Institute, Reporters without Borders and others work on a daily basis to provide resources to human rights and democracy activists, and journalists. Frontline Defenders provides an online training platform that helps to tailor security trainings to the needs to specific user communities. The Citizen Lab and Amnesty International have forensic capabilities to analyze mobile and other devices for potential malware and to examine the provenance of that malware. Despite all these resources currently available the threat of digital surveillance persists. What can these organizations do to better get the word out about digital surveillance? How might you and others within your own networks share information on the potential dangers arising from digital surveillance technologies? What other ways can you and these organization fight to protect against spyware and similar pernicious forms of malware.

Reflecting on The Pocket Assassin

> *"So, if your aim is to get inside someone's device without their permission and gather up information, you could do that using a very sophisticated commercial spyware technology like Pegasus. The latest iteration of it employs zero click technology meaning that it can target and insert itself on any device without the owner of that device even knowing or being tricked into clicking on a link. That's very powerful, because there is no defense against it."*
>
> ~ Ronald Deibert, Director of the Citizen Lab at the University of Toronto.

> *"Whoever can pierce your privacy can humiliate you and disrupt your relationships at will. No one (except perhaps a tyrant) has a private life that can survive public exposure by hostile directive."*
>
> ~ Timothy Snyder, On Tyranny Graphic Edition: Twenty Lessons from the Twentieth Century

The fight for human rights has been steadily progressing since the end of World War II. The Universal Declaration of Human Rights (1948), and a bevy of additional documents have slowly established a norms-based order that recognizes basic forms of human dignity. The fight for human rights in physical spaces is far from over. Countries such as Saudi Arabia, North Korea, Iran, and many others continue to violate human rights norms. Previously these violations were

principally conducted through physical means alone. Surveillance of activists once required large internal security services. Yet, just as activists have made use of digital devices to connect and leverage network effects to harness the power of diverse and distributed crowds, repressive regimes are now increasingly using the digital technologies that underpin these technologies to surveil. The technical complexity and manner in which the NSO Group's Pegasus spyware was able to penetrate and exploit mobile devices places the average user at a substantial disadvantage. There is little hope that the average device user can understand or counter sophisticated attacks without substantial external assistance from NGOs.

Pegasus constitutes a dystopian tool suited to a future devoid of privacy. The ability to reach into the private spaces of individuals without their knowledge from around the world at any time will raise the costs of activism, journalism, and opposition politics. These technologies chill free speech. The issues at the heart of the case above and the Pegasus story more specifically are rooted in issues of accountability, privacy, and liberty.

Accountability: The development and sale of software is difficult to regulate. Unlike physical goods, the transmission of digital goods can often be accomplished without regard to borders. The use of software even where regulated can be hard to monitor. The NSO Group claims that it attempted to self-regulate the sale and distribution of its product only to customers seeking to use it for counter terrorism purposes. Despite these claims it is abundantly clear that the Pegasus spyware they developed and licensed was used well beyond this narrow use case. There have been clear attempts by the U.S. and European governments to constrain the sale and use of Pegasus against their citizens. NSO Group even claimed that no U.S. persons were targeted. Yet this is naïve. Contained within the dataset of 50,000 persons were many Americans who had telephone numbers outside of the United States. The Israeli government had little incentive to regulate the NSO Group because it was both a regulator and a customer of its products. The result is that the NSO Group was subject to little real accountability. The mobile software and hardware firms whose products were exploited were similarly largely unaccountable for longstanding vulnerabilities. It took substantial investigative reporting and public shaming to force them to change their behaviors.

All is not lost. The physical infrastructures necessary for Pegasus to function is extensive and crosses multiple jurisdictional boundaries. Some of the jurisdictions in which the command-and-control systems were used could apply existing regulatory frameworks to prevent its use or could bring charges or fine companies or other entities that host such products. Pegasus is simply the largest and most complex version of Spyware to date. Holding all the actors in the development and sale of the software accountable would send an ecosystem-wide signal that surveillance is not acceptable without valid legal cause. If states are unable to hold companies such as the NSO Group accountable they are even less likely to hold smaller firms that produce stalkerware accountable. Ensuring that all actors in this space are held accountable is critical for the protection of basic human rights.

> *Historically, privacy was almost implicit, because it was hard to find and gather information. But in the digital world, whether it's digital cameras or satellites or just what you click on, we need to have more explicit rules - not just for governments but for private companies.*
>
> *~ Bill Gates*

Privacy: Article 12 of the Universal Declaration of Human Rights 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." This article outlines privacy as a fundamental human right. It is a human right because in many ways privacy can and does serve as the foundation for other forms of rights. The right to privacy is a bulwark against an aggressive and overreaching state. Privacy protects individuals from a dystopian future in which they are unable to act freely without interference. Human and democracy rights activists often require privacy to mobilize or organize. In the absence of privacy, the state can rapidly stifle such efforts before they can even begin to utilize the mobilizing network effects of modern technologies. If there is a concern that the state can read, watch, and track every movement then it becomes increasingly necessary to conform to the whims of the state. One only need read George Orwell's *1984* and his use of the term 'newspeak' to understand the deleterious consequences of a world devoid of privacy. It is a common assumption that looking at a screen in the conform of one's home, car, or office makes the actions private. But the case above makes clear that these actions taking place miles or even continents away from hostile prying eyes does not make them private. Pegasus invades the privacy of mobile phone users regardless of their location and it is unsparing in its violation of their privacy.

Liberty: The concept of liberty is not often included in these case analyses. Instead, the focus usually centers on equity, equality, accountability, or similar concerns. But the use of malware to violate the private spaces of individuals impedes upon their fundamental liberty. Spyware and stalkerware undermine Article 13 of the Universal Declaration of Human rights which established the right to the freedom of movement. Because Pegasus and other forms of spyware track a user's movements, they are in effect constraining the right to freedom of movement. By combining tracking information with private information on the proposed destination of an individual, these programs can and do place them in flexible digital jail cells of surveillance. In the case of Jamal Khashoggi, it provided sufficient information to set up a kill squad to lay in wait for him to arrive at the Saudi consulate. The definition of liberty is freedom from oppressive restrictions on one's way of life, behavior, or political views.[16] Spyware and stalkerware form an

[16] https://www.merriam-webster.com/dictionary/liberty

invisible cage that constrain and impose arbitrary and often unknown limits on an individual. At times these limits become self-reinforcing when targets of frequent surveillance self-censor or must curtail certain activities or behaviors. Worse yet these constraints are imposed across sovereign jurisdictional boundaries.

The tale of Jamal Khashoggi is hard to hear. The subsequent investigations into the pervasiveness of the Pegasus spyware and its use on thousands of individuals around the world sheds light on an often-overlooked attribute of a device carried by most individuals in their daily lives. The phone that entertains, captures our memories, holds our financial information, and our medical histories can also be a silent assassin wielded by hostile forces who wish us harm.

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

Brantly, Aaron, Nerea Cal, and Devlin Winkelstein. "Defending the Borderland: Ukrainian Military Experiences with IO, Cyber, and EW." West Point, NY: United States Army Cyber Institute, December 1, 2017. http://www.dtic.mil/dtic/tr/fulltext/u2/1046052.pdf.

"Forensic Methodology Report: How to Catch NSO Group's Pegasus." London, UK: Amnesty International, July 18, 2021. https://www.amnesty.org/en/documents/doc10/4487/2021/en/.

Freedom House. "Freedom in the World 2023 - Saudi Arabia," 2023. https://freedomhouse.org/country/saudi-arabia/freedom-world/2023.

Jee, Charlotte. "How 'Stalkerware' Apps Are Letting Abusive Partners Spy on Their Victims." *MIT Technology Review*, July 10, 2019. https://www.technologyreview.com/2019/07/10/134249/stalkerware-apps-are-letting-abusive-partners-spy-on-their-victims/.

Jones, Sam. "Pegasus Spyware Used in 'Jaw-Dropping' Phone Hacks on El Salvador Journalists." *The Guardian*, January 13, 2022. https://www.theguardian.com/news/2022/jan/13/pegasus-spyware-target-journalists-activists-el-salvador.

Kirchgaessner, Stephanie. "Mexico: Reporters and Activists Hacked with NSO Spyware despite Assurances." *The Guardian*, October 4, 2022. https://www.theguardian.com/world/2022/oct/04/mexico-nso-spyware-journalists-human-rights-hacked-pegasus.

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/.

Priest, Dana, Souad Mekhennet, and Arthur Bouvart. "Jamal Khashoggi's Wife Targeted with Spyware before His Death." *The Washington Post*, July 18, 2021. https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/.

Shezaf, Hagar. "Snowden: Israeli Firm's Spyware Was Used to Track Khashoggi." *Haaretz*, November 7, 2018. https://www.haaretz.com/israel-news/2018-11-07/ty-article/.premium/israeli-spyware-was-used-to-track-saudi-journalist-khashoggi-edward-snowden-says/0000017f-e09f-df7c-a5ff-e2ffc1650000.

Staff, Washington Post. "Takeaways from the Pegasus Project." *The Washington Post*, August 2, 2021. https://www.washingtonpost.com/investigations/2021/07/18/takeaways-nso-pegasus-project/.

Weiting, Ayse, and Suzan Fraser. "Turkish Court Moves Trial of 26 Saudis Suspected of Gruesome Khashoggi Killing to Saudi Arabia." *PBS*, April 22, 2022. https://www.pbs.org/newshour/world/turkish-court-moves-trial-of-26-saudis-suspected-of-gruesome-khashoggi-killing-to-saudi-arabia.

Zetter, Kim. "Pegasus Spyware: How It Works and What It Collects." *Zero Day*, August 4, 2021. https://zetter.substack.com/p/pegasus-spyware-how-it-works-and?utm_source=%2Fsearch%2Fpegasus&;utm_medium=reader2.