IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

HANAN ELATR KHASHOGGI

Plaintiff,

v.

NSO GROUP TECHNOLOGIES LIMITED

and

Q CYBER TECHNOLOGIES LIMITED,

22 Galgalei Haplada, Herzliya, Tel Aviv-Yafo,
Israel 4672222

Defendants.

Civil Action No. 1:23-cv-779

COMPLAINT

JURY TRIAL DEMANDED

Hanan Elatr Khashoggi ("Hanan" or "Plaintiff"), by and through undersigned counsel, alleges the following against Defendants NSO Group Technologies Limited ("NSO Group") and Q Cyber Technologies Limited ("Q Cyber") (collectively, "NSO Group" or "Defendants"):

I. INTRODUCTION

1. Defendants have long infringed upon the basic principles of personal freedom and the fundamental right to privacy through the creation, sale, and operation of highly sophisticated and malicious spyware. Those actions can—and have—resulted in disastrous outcomes, including intimidation, physical injury, and death. For Hanan Khashoggi, the ramifications of Defendants' exploits have tragically played out before her eyes, forever altering her life.

2. NSO Group and its parent company, Q Cyber, create, market, and sell spyware and provide technical assistance and consulting to government clients that contract with them to use their spyware. Often, these clients were known authoritarian regimes working with NSO Group to use its spyware to target anyone who poses a perceived "threat" to the reigning power. Targeted persons deemed "threats" include not just criminals, but also activists, humanitarians, dissidents, and journalists. Unfortunately, the nefarious use of the spyware does not stop there—NSO Group technology is also used to track the friends, family members, and loved ones of anyone the client deems suspicious.

3. Defendants' actions have drawn criticism—and intense fear—from reporters and activists targeted by the spyware, as well as from politicians, government officials, and the technology industry at large. Shane Huntley, Director of Google's Threat Analysis Group ("TAG") testified in front of the U.S. House Committee on Intelligence, gravely summarizing:

> While these vendors claim to vet their customers and usage carefully with the promise that the work is used to counter criminals and terrorists, what we have observed in TAG is consistent with others' reporting—that again and again these tools are found to be used by governments for purposes antithetical to democratic values, targeting dissidents, journalists, human rights workers, and political

> opponents. NSO Group is the most prominent actor offering spyware and these services. . . .[1]

4. Hanan Khashoggi suffered through the brutal kidnapping and murder of her husband, Jamal Khashoggi, at the hands of Saudi Arabian actors sent by the Crown Prince of Saudi Arabia, Mohammed bin Salman, assisted by allies in the United Arab Emirates. While she was still mourning her husband's death, in addition to dealing with the violent nature of the killing and international publicity surrounding it, she was hit with another disturbing revelation. For nearly a year leading up to Jamal's murder, Hanan's phones had been infiltrated by NSO Group spyware.

5. Hanan was then left to deal with the knowledge that her husband's life was cut short by Saudi agents who perpetuated the killing, using, upon information and belief, knowledge about Jamal obtained by NSO Group from Hanan's own devices, which were transformed into handheld spies.

II. THE PARTIES

<u>PLAINTIFF</u>

6. Plaintiff Hanan Elatr Khashoggi is an Egyptian citizen and the widow of Jamal Khashoggi. Plaintiff is a lawful resident of the United States and is currently seeking the status of political asylum in the United States.

7. Plaintiff brings this action on her own behalf.

8. Jamal Khashoggi was a prominent and prolific writer, editor, and activist who was well-known for his thoughtful opinions on the rights of women and other minorities, and his calls for governmental reform in Saudi Arabia and the Middle East at-large.

9. Hanan currently resides in the Commonwealth of Virginia. Before her husband Jamal's death, Hanan shared a home with him in Fairfax County, Virginia. She is currently legally employed through a work visa and is working and living full-time in Virginia.

[1] *Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware Before the U.S. House of Representatives, Permanent Select Committee on Intelligence*, 117th Cong. (2022).

10. Hanan was employed as a flight attendant for Emirates Airlines for more than twenty years.

11. Hanan and Jamal met at a conference in the United Arab Emirates ("UAE") in 2009, and Hanan became Jamal's confidante and friend. The two communicated by phone, staying in touch for years before their relationship became romantic.

12. As detailed herein, Jamal eventually had reason to fear for his safety in Saudi Arabia, and was forced to flee Saudi Arabia in the summer of 2017. Once in the United States, Jamal reached out to Hanan and invited her to reconnect with him in his new home in Virginia.

13. After accepting Jamal's invitations, the two quickly began dating, and not long after began contemplating marriage. Jamal proposed to Hanan in April 2018.

14. Shortly after the proposal, in the course of her usual flight schedule, Hanan arrived in Dubai. However, this time, she was greeted at the airport by UAE intelligence officials that confiscated her devices, questioned, and detained Hanan for two weeks.

15. In June 2018, the couple was married by an Imam in an Islamic ceremony in Virginia. After their wedding, the newlyweds lived in their shared Tysons Corner, Virginia condominium as husband and wife.

16. In October 2018, Hanan and Jamal's story came to a violent end when Jamal was assassinated in the Saudi Arabian consulate in Istanbul for his writings and critiques of the Saudi regime.

17. After the murder of her husband, Hanan lost her job after experiencing continued harassment from the government of the UAE, including being interrogated and held against her will—again—for more than two months in early 2019. The UAE, the Kingdom of Saudi Arabia, and other actors have closely monitored and intimidated Jamal's loved ones even after his death.

18. Due to the actions of Defendants and their clients, Hanan is now seeking the protections of political asylum in the United States.

19. Continuing the advocacy that her husband began, Hanan has spoken out against the actors responsible for causing Jamal's death and seeks justice for him and on her own behalf through this action.

DEFENDANTS

20. Defendant NSO Group Technologies Limited is a limited liability company incorporated in Israel on January 25, 2010. NSO Group created, developed, sold, and assisted in the deployment and use of cutting-edge spyware technology to clients around the world.

21. Defendant NSO Group is a subsidiary of Q Cyber Technologies, and upon information and belief, sometimes conducts business under that moniker.

22. Defendant Q Cyber Technologies Limited is a limited liability company incorporated in Israel on December 2, 2013 under the name L.E.G.D. Company Limited. The company officially changed its name to Q Cyber Technologies on May 29, 2016. Q Cyber is the parent company of NSO Group and a subsidiary of OSY Technologies SARL.

23. Upon information and belief, NSO Group and Q Cyber Technologies are currently managed, in all material respects, by one of their founders, Omri Lavie.

24. Upon information and belief, Omri Lavie registered Dufresne Holding, a limited liability company, in Luxembourg on or about February 2023.

25. Upon information and belief, at the time of its registration Dufresne Holding had one shareholder, Omri Lavie.

26. Upon information and belief, on or around April 2023 Dufresne Holding became the sole shareholder of NorthPole Newco S.a.r.l.

27. Upon information and belief, NorthPole Newco S.a.r.l was the sole shareholder of OSY Technologies S.a.r.l at the time Dufresne Holding became the sole shareholder of NorthPole Newco S.a.r.l.

28. Upon information and belief, the ownership and management of NSO Group and Q Cyber through groups based in Luxembourg consisted, at one time or another, of up to seven

other companies: Triangle Holdings, Square 2, Novalpina Capital Partners, Novalpina Capital Group, Northpole Holdco, NorthPole Bidco and NorthPole Newco.[2]

29. Defendants intentionally targeted the devices of Hanan Khashoggi and caused her immense harm, both through the tragic loss of her husband and through her own loss of safety, privacy, and autonomy, as well as the loss of her financial stability and career.

30. In addition to intentionally targeting Hanan (and through Hanan, Jamal) and her devices in Virginia, NSO Group also has significant ties to the United States. For much of the past decade, NSO Group has been primarily funded and controlled by California-based investment funds and has engaged the U.S. government (and local governments within the U.S.) as potential clients.[3] Further, NSO Group has a U.S. subsidiary company, Westbridge Technologies, Inc. that is headquartered in Virginia. NSO Group created Westbridge to help market and sell Defendants' spyware to the U.S. market.

31. Even after being placed on a restricted entity list by the United States Department of Commerce, NSO Group has continued to aggressively lobby its services in the United States, and upon information and belief, continues that lobbying today.[4] In 2022 alone, "NSO Group paid

[2] *See* Cordula Schnuer, "Nine NSO entities in Luxembourg, minister confirms," *Delano*, July 21, 2021, https://delano.lu/article/nine-nso-entities-in-luxembour (last accessed June 5, 2023); *see also* Stephanie Kirchgaessner, "NSO Group co-founder emerges as new majority owner," *The Guardian*, March 1, 2023, https://www.theguardian.com/technology/2023/mar/01/one-of-nso-groups-founders-emerges-as-new-majority-owner (last accessed June 5, 2023).

[3] Mark Mazzetti and Ronen Bergman, "Internal Documents Show How Close the F.B.I. Came to Deploying Spyware," *New York Times,* November 12, 2022, https://www.nytimes.com/2022/11/12/us/politics/fbi-pegasus-spyware-phones-nso.html (stating that FBI officials "made a push in late 2020 and the first half of 2021 to deploy the hacking tools—made by the Israeli spyware firm NSO—in its own criminal investigations.") (last accessed June 5, 2023); *see also* Joseph Cox, "LAPD Got Tech Demos from Israeli Phone Hacking Firm NSO Group," *Vice*, June 9, 2020, https://www.vice.com/en/article/n7wna7/lapd-phone-hacking-nso-group-westbridge (stating that members of the Los Angeles Police Department received a demo of Pegasus from NSO Group) (last accessed June 5, 2023).

[4] Inci Sayki, "Spyware firm NSO Group Continues Lobbying Efforts to Resume Business-as-Usual in the U.S.," *OpenSecrets.org*, May 15, 2023, https://www.opensecrets.org/news/2023/05/spyware-firm-nso-group-continues-lobbying-efforts-

over $1.1 million to public relations companies and law firms in the U.S. . . ., more than the government of Israel . . . spent in total on its U.S. lobbying operation through the same period. . . . Since 2020, NSO Group has paid foreign agents more than $2.9 million for foreign influence and lobbying operations in the U.S."[5]

32. Upon information and belief, at all times material to this case, each Defendant was the agent, partner, alter ego, subsidiary, parent, and/or co-conspirator of and with the other Defendant, and the acts of each Defendant were within the scope of that relationship; each Defendant knowingly and intentionally agreed with the other to carry out the acts alleged in this Complaint; and in carrying out the acts alleged in this Complaint, each Defendant acted with the knowledge, permission, and consent of the other, and each Defendant aided and abetted the other.

III. JURISDICTION AND VENUE

33. This Court has jurisdiction over Plaintiff's federal causes of action pursuant to 28 U.S.C. § 1331 because these causes of action arise under federal law—the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. This Court has subject matter jurisdiction over Plaintiff's claims under the Virginia Computer Crimes Act, Va. Code § 18.2-152.1, *et seq*., claims of Trespass to Chattels, Negligence, Intentional Infliction of Emotional Distress, Negligent Infliction of Emotional Distress, and claims for equitable relief pursuant to 28 U.S.C. § 1367 because these claims arise out of the same nucleus of operative fact as Plaintiff's federal law claims.

34. This Court has personal jurisdiction over Defendants because Defendants engaged in conduct within the Commonwealth of Virginia, resulting in sufficient minimum contacts with this forum. Defendants have utilized instrumentalities located in Virginia (Plaintiff's personal devices) as well as targeting residents of Virginia (Hanan and Jamal Khashoggi) specifically, with

to-resume-business-as-usual-in-the-u-s#:~:text=NSO%20Group%20paid%20over%20%241.1,operation%20through%20the%20same%20period (last accessed June 5, 2023).

[5] *Id.*

knowledge that such targeting would result in significant harm to Plaintiff in Virginia and violate the laws of the United States.

35. This Court also has personal jurisdiction over Defendants under the "effects" test set forth in *Calder v. Jones*, 465 U.S. 783 (1984) because Defendants have committed an intentional tort, Plaintiff suffered the harm of that act in this forum, and Defendants expressly aimed their tortious conduct at the Plaintiff in Virginia such that Virginia can be said to be the focal point of the tortious activity.

36. Personal jurisdiction is proper under Virginia's long-arm statute, Va. Code Ann. § 8.01-328.1, which provides that a court may exercise personal jurisdiction over a party as to a cause of action arising from the party (a) transacting any business in Virginia, (b) causing tortious injury by an act or omission in Virginia, or (c) causing tortious injury in Virginia by an act or omission outside Virginia if the party regularly does or solicits business, or engages in any other persistent course of conduct, or derives substantial revenue from goods used or consumed or services rendered, in Virginia. Pursuant to the long-arm statute, using a computer or computer network located in Virginia constitutes an act in Virginia. Defendants are therefore subject to personal jurisdiction in Virginia because they caused tortious injury to the Plaintiff in Virginia when they infiltrated and continuously monitored Plaintiff through her devices while she lived in Virginia with her husband. Defendants are located in Israel and Defendants have gained substantial revenue by providing services to their clients, with knowledge that those clients were then likely to target individuals residing in the United States.

37. Alternatively, this Court has personal jurisdiction over Defendants pursuant to Federal Rule of Civil Procedure 4(k)(2).

38. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(2) or, alternatively, 28 U.S.C. § 1391(b)(3).

IV. FACTUAL ALLEGATIONS

THE WORLD'S MOST POWERFUL SPYWARE—NSO GROUP'S "PEGASUS"

39. NSO Group has made its name amongst authoritarian governments and those known for perpetuating human rights abuses by offering them "Pegasus," the world's most powerful, sophisticated, and infamous cyberweapon.[6]

40. Pegasus is an advanced surveillance tool designed to be undetectable—it evades traditional security measures and is installed on the user's device without their knowledge or consent. Further, Pegasus can remotely infect a target's cell phone using a simple text message.

41. The version of Pegasus installed on Plaintiff's phone was in high demand due to its unique remote "zero click" feature. That is, no interaction was required by the target to have their phone compromised. Most available spyware requires some interaction by the target, such as clicking a link or opening a file. With Pegasus, NSO Group needed only the target's phone number, and it could then see "every piece of data stored on the phone."[7]

42. Forensic investigation performed by Citizen Lab, a research laboratory based out of the University of Toronto's Munk School of Global Affairs, provided evidence that both of Plaintiff's Android phones were infected with Pegasus by April 2018, and likely earlier, with

[6] Upon information and belief, Pegasus has been sold to the Governments of Ghana, Rwanda, and the United Arab Emirates, despite the questionable human rights records of each. Stephanie Kirchgaessner and Diane Taylor, "Nephew of jailed Hotel Rwanda Dissident hacked by NSO Spyware," *The Guardian*, July 18, 2022, https://www.theguardian.com/world/2022/jul/18/nephew-of-jailed-hotel-rwanda-dissident-hacked-by-nso-spyware (last accessed June 5, 2023); *see also* 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 (last accessed June 5, 2023); Omer Benjakob, "NSO Ghana Op Exposed: Never-before-seen Pegasus Spyware Footage, Workers' Passports," January 20, 2022, https://www.haaretz.com/israel-news/tech-news/2022-01-20/ty-article/nso-ghana-op-exposed-never-before-seen-pegasus-spyware-footage-workers-passports/0000017f-f1fb-df98-a5ff-f3ffb9a20000 (last accessed June 5, 2023).

[7] 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 (last accessed June 5, 2023).

attempts on her devices dating back to November 2017.[8] The infiltration allowed for all information stored on Plaintiff's phones to become accessible. However, it also granted access to all future phone calls, communication activity through apps, and text messages in perpetuity. Further, the infiltration gave Defendants and Defendants' client(s) the ability to activate the cameras and microphones of Plaintiff's phones without her knowledge, turning her phones into sophisticated listening and recording devices.[9]

43. Because of the unique danger posed by Pegasus and NSO Group, the United States Commerce Department's Bureau of Industry and Security placed NSO Group on its Entity List based on evidence that it "developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers."[10] Defendants' activity has resulted in countless human rights violations and is an urgent matter of national security.

44. John Scott-Railton, a Senior Researcher at the Citizen Lab,[11] addressed the pernicious nature of the industry in front of the U.S. House Intelligence Committee:

> When confronted with abuses the mercenary spyware industry typically has a message: Our technology is designed to fight crime

[8] *See infra* section IV.

[9] Dana Priest, "A UAE Agency put Pegasus spyware on phone of Jamal Khashoggi's wife months before his murder, new forensics show," *Washington Post*, December 21, 2021, https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/.

[10] U.S. Department of Commerce, "Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities," November 3, 2021, https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list (last accessed June 5, 2023).

[11] Citizen Lab has been at the forefront of researching and sounding the alarm on NSO Group and other mercenary spyware companies. Citizen Lab analyzed the devices of Hanan Khashoggi for evidence of NSO Group activity and has done so for countless others as the go-to organization for detection of the extremely sophisticated spyware. According to its website, "The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security." *See* "About the Citizen Lab" https://citizenlab.ca/about/ (last accessed June 9, 2023).

> and terror. Period. But the facts don't bear this out, in two ways. ***First, abuses have been a feature of this technology and industry since day one***. Second, and as we have discussed today, the crime and terror narrative omits the fact that a significant proportion of the use that we see of mercenary spyware is state-on-state espionage, governments targeting other governments. And of course the United States has been one of those targets.[12]

45. NSO Group publicly states that it takes a hands-off approach after selling its powerful spyware to authoritarians, and that it offers no assistance to its clients after the transaction is complete.[13]

46. However, those statements are simply not true. NSO Group stays intimately involved in the surveillance process after providing its tools to its clients, with representatives explicitly stating, "we hear about…every phone call that is being hacked over the globe, ***we get a report immediately***."[14]

47. Also contrary to its prior assertions, NSO Group itself has boasted that it offers clients "cyber intelligence, data acquisition, ***and analysis***."[15]

[12] *Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware Before the U.S. House of Representatives, Permanent Select Committee on Intelligence*, 117th Cong. (2022) (emphasis added).

[13] In a post titled "Enough is Enough!" NSO Group's website states its repetitive claim for plausible deniability: "NSO is a technology company. We do not operate the system, nor do we have access to the data of our customers, yet they are obligated to provide us with such information under investigations." NSO News, Enough is Enough, NSO Group, https://web.archive.org/web/20230323182216/https://www.nsogroup.com/Newses/enough-is-enough/ (last accessed June 5, 2023).

[14] Ronan Farrow, "How Democracies Spy on their Citizens," *The New Yorker*, April 18, 2022, https://www.newyorker.com/magazine/2022/04/25/how-democracies-spy-on-their-citizens (last accessed June 5, 2023) (emphasis added).

[15] 2019 ISS World Europe—Lead Sponsor, *TeleStrategies ISS World Europe*, https://web.archive.org/web/20190908051829/https://www.issworldtraining.com/iss_europe/sponsors.html (last accessed June 5, 2023) (emphasis added).

48. A sales brochure for Pegasus, also filed in *WhatsApp v. NSO Group*, further outlines tactics that NSO Group suggests its clients use to infiltrate target phones.[16]

49. Upon information and belief, NSO Group describes two remote "installation vectors" for Pegasus: Remote installation ("over-the-air" or "OTA") and Enhanced Social Engineering Messages ("ESEM").

50. Social engineering, in the cybersecurity context, refers to a manipulative tactic to induce the target to provide their own vulnerabilities to a bad actor. One common example is phishing—where a website or email appears to be legitimate, but in fact is not, inducing the target to click on a link that exposes them to malware or spyware.

51. NSO Group states that the ESEM method allows "the system operator [to] choose to send a regular text message (SMS) or an email, luring the target to open it." NSO Group brags that a "[s]ingle click, either planned or unintentional, on the link will result in hidden agent installation."[17]

52. NSO Group further offers that "[t]he Pegasus solution provides a wide range of tools to compose a tailored and innocent message to lure the target to open the message."[18]

53. NSO Group clients have multiple options when deciding how to obtain a primary target's personal information. First, they can "direct target" the primary individual in question—for example, a journalist, human rights activist, or political refugee. Direct targeting may be utilized for individuals that have exploitable security gaps on their phone. The problem with this approach for NSO Group and its clients is that most of these "direct targets" know that they may be at risk of some sort of spyware and often are more vigilant in securing their devices.

[16] Exhibit 1 at 13 ("When physical access to the device is an option, the Pegasus agent can be manually injected and installed in less than five minutes."). *See generally* Compl., *WhatsApp Inc. v. NSO Group Technologies Limited*, 3:19-cv-07123 (N.D. Cal. Oct. 29, 2019), ECF No. 1.

[17] Exhibit 1 at 12.

[18] *Id.* at 13.

54. The way around this obstacle is to invoke a second option: utilization of what is known as "relational" or "off-center" targeting. Relational targeting is when "spouses, siblings, parents, staff, or close associates of primary targets [are] targeted and infected with Pegasus."[19] This allows NSO Group's clients to circumvent the security features that are typically utilized by hyper-vigilant primary targets, like Jamal Khashoggi.[20]

55. These two options are not mutually exclusive and can be deployed in tandem by the Pegasus operator to give the best chance of success in obtaining the personal details of the primary target.

56. Infecting a primary target's network of close, trusted associates allows NSO Group's clients to exploit the laxer security standards of individuals who would otherwise not fear targeting. Relational targeting also allows clients to develop contingency in the case that the primary target's phone cannot be hacked for technical reasons (*e.g.*, if the primary target is unable to be exploited). Even if the primary target infiltration is successful, having a relational target close to the direct target provides security for the client in the event that connection is disrupted (*e.g.*, by the target entering a country with a different network system). Finally, relational targeting also simply provides another avenue of unfiltered information both from the direct target him or herself and through what the relational target relays about the direct target to third parties.

[19] John Scott-Railton, Elies Campo, Bill Marczak, Bahr Abdul Razzak, Siena Anstis, Gözde Böcü, Salvatore Solimano, and Ron Deibert, *CatalanGate, Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Chandiru*, April 18, 2022 https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ (last accessed June 5, 2023).

[20] Jamal, referring to Crown Prince Mohammed bin Salman, reportedly told friends that "The kid is dangerous." Kristina Jovanovski and Saphora Smith, "Jamal Khashoggi was fearful of Saudi government before disappearing, friends say," *NBC News*, October 9, 2018, https://www.nbcnews.com/news/world/jamal-khashoggi-was-fearful-saudi-government-disappearing-friends-say-n917686 (last accessed June 5, 2023). Jamal shared his fears around his safety with Hanan, beginning at least in November 2016 after Jamal was critical of Donald Trump after he was elected President of the United States.

57. NSO Group knew, or should have known, that its clients routinely utilized relational targeting and that relational targeting was incredibly effective at accomplishing the goals of authoritarian regimes (*e.g.*, suppressing dissent and intimidating the public).

58. One clear example of this tactic played out in Catalonia, Spain, where political figures were targeted by Pegasus between 2017 and 2020. This was accomplished using a WhatsApp exploit, similar to one of the attempts on Hanan's phone.[21] At the time, political figures in Catalonia were campaigning for a fully independent Catalonia, which Spain's Constitutional Court maintained was contrary to law. Catalonia's former president, Carles Puigdemont, supported a binding referendum for citizens to vote on independence. In its investigation of the hacking of pro-independence politicians, Citizen Lab was not able to confirm that Puigdemont's phone was infected with Pegasus.

59. However, Citizen Lab concluded that "an arc of targeting" formed around Puigdemont. Eleven individuals ranging from Puigdemont's "spouse and residence staff to confidants, his lawyer, and friends" had their devices compromised.[22] Citizen Lab concluded that "monitoring their devices would have provided a detailed window into [Puigdemont's] life, movements, and thinking."[23]

60. NSO Group publicly contends that it can identify and stop any "misuse" of its weapon (such as the targeting of activists' family members).[24] However, upon information and

[21] Scott-Railton, "*CatalanGate, Extensive Mercenary Spyware Operation against Catalans Using Pegasus and Chandiru*" April 18, 2022 https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/ (last accessed June 5, 2023).

[22] https://catalonia.citizenlab.ca/#targeting-puigdemont (last accessed June 5, 2023) (emphasis added).

[23] *Id.*

[24] Audrey Travère, "The Rise and Fall of NSO Group," *Forbidden Stories*, July 19, 2021, https://forbiddenstories.org/the-rise-and-fall-of-nso-group/ (Co-founder Shalev Hulio states "We understand that in some circumstances our customers might misuse the system and, in some cases like we reported in the Transparency and Responsibility report, we have shut down system for customers who have misused the system.") (last accessed June 5, 2023).

belief, despite this claim, NSO Group has failed to do so, as evidenced by the number of times Pegasus has been used to spy on innocent individuals.

61. For example, in May 2017, Mexican journalist Javier Valdez was shot and killed outside of his office. Valdez had been investigating the Sinaloa cartel at the time. Days after Valdez was killed, his colleagues received carefully crafted text messages (another instance of the use of ESEM) that would infect their phones with Pegasus if they clicked on the contained links.[25]

62. Eleven days after Valdez was killed, his wife, Griselda Triana, was also targeted by ESEM links. Griselda received two messages specifically tailored to induce her to click on them and infect her phone with Pegasus.

63. Citizen Lab concluded that the operator attempting to install Pegasus onto Valdez's wife and colleagues' phones was active until 2017. Citizen Lab further concluded that the operator was the Mexican Government. The Mexican Government's original infrastructure (dubbed 'RECKLESS-1' by Citizen Lab) was disabled in June 2017. However, while RECKLESS-1 was not re-enabled, Citizen Lab concluded that the Mexican Government continued operating Pegasus infrastructure.[26]

64. Upon information and belief, given RECKLESS-1's closure, and the Mexican Government's subsequent use of Pegasus infrastructure, NSO Group knew or should have known at least as early as 2017 that its cyberweapon was used to target colleagues and spouses of journalists and activists. Despite this early evidence of NSO Group's actual or constructive

[25] John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "Reckless VII, Wife of Journalist Slain in Cartel-Linked Killing Targeted with NSO Group's Spyware," Citizen Lab Research Report No. 117, University of Toronto, March 20, 2019, https://citizenlab.ca/2019/03/nso-spyware-slain-journalists-wife/ (last accessed June 5, 2023).

[26] John Scott-Railton, Bill Marczak, Siena Anstis, Bahr Abdul Razzak, Masashi Crete-Nishihata, and Ron Deibert, "New Pegasus Spyware Abuses Identified in Mexico," Citizen Lab Research Report No. 78, University of Toronto, October 2, 2022, https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/ (identifying infections against journalists from 2019-2021) (last accessed June 5, 2023).

knowledge of Pegasus's usefulness in targeting journalists via their friends and family, it did nothing to prevent Jamal Khashoggi's wife, Hanan, from being targeted the following year.

65. To summarize, NSO Group outlines three technical options for its clients to gain total control of a device: (1) remote, zero-click entry via software exploit; (2) physical installation on the device; and/or (3) inducing the target to unwittingly install Pegasus on their device via ESEM. To maximize the chance of successful infiltration, clients can utilize one or more of these methods. For example, Citizen Lab found evidence that the Pegasus software was installed via physical installation on Hanan's phones ***and*** that she received a number of malicious ESEM texts containing links that would also install Pegasus on her phones. Upon information and belief, deployment of these three techniques often goes beyond the direct target, and targets include family members and close confidants.

66. Upon information and belief, in addition to its design and sale of spyware, NSO Group offers four levels of support to its clients after selling Pegasus to them.

67. The first level of technical support ("Tier 1") provides an engineer trained by NSO Group who can assist with, *inter alia*, "basic troubleshooting, configuration changes, and/or operation optimization."[27]

68. Tier 2 support provides technical support via an NSO Group "Field Service Engineer" who provides, *inter alia*, "advanced troubleshooting."[28]

69. Tier 3 support is provided by an NSO Group "Technical Support Specialist" who can provide, *inter alia*, "how to" support.[29]

70. Tier 4 support is provided by an NSO Group "R&D Engineer" who can support, *inter alia*, "design level consultation and solutions."[30]

[27] Compl. at 108, *WhatsApp Inc. v. NSO Group Technologies Limited*, 3:19-cv-07123 (N.D. Cal. Oct. 29, 2019), ECF No. 1-1 (Exhibit 11 to *WhatsApp* Complaint).

[28] *Id.*

[29] *Id.*

[30] *Id.*

71. NSO Group also provides phone and email support and a helpdesk that is available 24 hours a day, 7 days a week.[31]

NSO GROUP'S REPEATED SALES TO THE UAE AND OTHER COUNTRIES NOTORIOUS FOR VIOLATIONS OF BASIC HUMAN RIGHTS

72. Ahmed Mansoor is a human rights activist based in the UAE. Upon information and belief, in 2016, Ahmed Mansoor received personalized text messages consistent with NSO Group's ESEM tactics encouraging him to click on a link. Rather than clicking, Mansoor sent the messages to Citizen Lab.

73. The link would have jailbroken Mansoor's iPhone and turned it into a 24/7 spy-device that he took with him everywhere he went.

74. Investigation by Citizen Lab confirmed that the most likely operator behind Mansoor's targeting was the UAE Government. Mansoor had been the target of the UAE several years earlier and was imprisoned in his home country for eight months in 2011.

75. Despite the UAE's prior targeting of human rights activists—including Mansoor—NSO Group, upon information and belief, sold its Pegasus software to the UAE in 2016.[32]

76. Not to be dissuaded by their client's use of the world's most powerful cyberweapon to spy on activists, NSO Group continued to sell its products and services to the UAE. According to reports, the UAE had been using Pegasus for more than a year when NSO Group tried to upsell them on a new update.

77. Intrigued by the promise of an updated Pegasus, the UAE challenged Defendants to hack the phone of an editor of a London-based Arab newspaper. In order to push its new product, NSO Group agreed to actively participate in illegally surveilling Abdulaziz Alkhamis. Days later, an NSO Group representative supplied recordings of the editor's phone calls to UAE officials.

[31] *Id.*

[32] Bill Marczak & John Scott-Railton, "The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender," Citizen Lab Research Report No. 78, University of Toronto, August 24, 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (last accessed June 5, 2023).

Abdulaziz Alkhamis later confirmed that he had no idea that he was under surveillance by Defendants.[33] Defendants actively initiated spying on a journalist simply to showcase Pegasus's frightening capabilities.

78. Despite the UAE's use of Pegasus to surveil Ahmed Mansoor, and its subsequent request (and NSO Group's compliance) to illegally surveil a journalist based in the United Kingdom, NSO Group continued to sell its software to the UAE.[34] Even without NSO Group's knowledge of, and participation in, these illegal uses of its product, NSO Group claims to vet its clients before engaging with them—specifically looking for evidence of human rights abuses.[35] However, the UAE, and several of NSO Group's other suspected clients, have well-documented and long-standing histories of human rights abuses.[36]

79. Indeed, the UAE is not the only country with well-documented human rights violations with whom NSO Group eagerly partnered.

[33] David D. Kirkpatrick and Azam Ahmed, "Hacking a Prince, an Emir and a Journalist to Impress a Client," *The New York Times*, August 31, 2018, https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html

[34] *Id.*

[35] *See NSO News*, NSO Group, https://www.nsogroup.com/Newses/following-the-publication-of-the-recent-article-by-forbidden-stories-we-wanted-to-directly-address-the-false-accusations-and-misleading-allegations-presented-there/ (last accessed June 6, 2023) ("We would like to emphasize that NSO sells it technologies solely to law enforcement and intelligence agencies of vetted governments for the sole purpose of saving lives through preventing crime and terror acts.").

[36] U.S. Dep't of State, Bureau of Democracy, H.R. and Lab., 2018 Country Reports on Human Rights Practices: United Arab Emirates, 2018. *Available at:* https://www.state.gov/wp-content/uploads/2019/03/UNITED-ARAB-EMIRATES-2018.pdf (In 2018, the U.S. Department of State found that human rights abuses in the UAE included: "allegations of torture in detention; arbitrary arrest and detention, including incommunicado detention, by government agents; political prisoners; government interference with privacy rights; undue restrictions on free expression and the press, including criminalization of libel, censorship, and internet site blocking; substantial interference with the rights of peaceful assembly and freedom of association; the inability of citizens to choose their government in free and fair elections; and criminalization of same sex sexual activity.").

80. Rwandan activist Carine Kanimba's phones were targeted by the Rwandan government in September 2020 and July 2021 using NSO Group's spyware.[37] Carine is the daughter of notable human rights activist Paul Rusesabagina.

81. In 2021 the U.S. State Department noted "significant human rights issues" including credible reports of:

> unlawful or arbitrary killings by the government; forced disappearance by the government; torture or cruel, inhuman, or degrading treatment or punishment by the government; harsh and life-threatening prison conditions; arbitrary detention; political prisoners or detainees; politically motivated reprisals against individuals located outside the country, including killings, kidnappings, and violence; arbitrary or unlawful interference with privacy; serious restrictions on free expression and media, including threats of violence against journalists, unjustified arrests or prosecutions of journalists, and censorship.[38]

82. Carine Kanimba told a U.S. House Intelligence Committee that "[t]he same government that tortured my father, that is holding him hostage, and that has been trying to silence him all these years now also has access to my private messages and my conversations and my location, it is very, very scary."[39]

83. NSO Group also contracted to provide its Pegasus infrastructure to Ghana in 2016. The Ghanaian government allegedly "planned to use Pegasus to snoop on opposition figures ahead

[37] Antoaneta Roussi, "Daughter of imprisoned Rwandan dissident: Governments must be 'accountable' for spyware use," *Politico*, July 28, 2022, https://www.politico.eu/article/carine-kanimba-rusesabagina-daughter-imprisoned-rwanda-dissident-government-accountable-spyware-use/ (last accessed June 5, 2023).

[38] U.S. Dep't of State, Bureau of Democracy, H.R. and Lab., 2021 Country Reports on Human Rights Practices: Rwanda, 2021. *Available at:* https://www.state.gov/reports/2021-country-reports-on-human-rights-practices/rwanda/.

[39] *Combatting the Threats to U.S. National Security from the Proliferation of Foreign Commercial Spyware Before the U.S. House of Representatives, Permanent Select Committee on Intelligence*, 117th Cong. 25 (2022). (statement of Carine Kanimba, Target of Foreign Commercial Spyware).

of a 2017 election."[40] Employees of NSO Group reportedly traveled to Ghana and trained locals how to use it.[41]

84. The U.S. State Department noted in 2016 that Ghana's human rights abuses included "…excessive force by police, including torture that resulted in death and injuries; harsh and life-threatening prison conditions; trafficking in persons; and exploitative child labor, including forced child labor."[42]

85. Notably, the State Department also assessed that there was "corruption in all branches" of Ghana's government.[43]

NSO GROUP'S ROLE IN THE DEATH OF JAMAL KHASHOGGI

86. Jamal Ahmid Khashoggi was a prominent and prolific Saudi Arabian journalist and activist. His work over the span of his career impacted the cultural and political landscape throughout the Middle East. While Jamal considered himself a "moderate," much of his work was at the forefront of forward-thinking philosophies and ideals, even when those points of view put him at odds with powerful people.

87. Jamal was an intrepid journalist throughout the 1980s and was the editor of *Al Madina* magazine from 1991 to 1999. Jamal went on to become the Deputy Editor-in-Chief of *Arab News*, one of the most prominent newspapers in Saudi Arabia, and subsequently became the Editor of *Al-Watan*, a position he was terminated from only two months later after running afoul

[40] Omer Benjakob, "NSO Ghana Op Exposed: Never-before-seen Pegasus Spyware Footage, Workers' Passports," January 20, 2022, https://www.haaretz.com/israel-news/tech-news/2022-01-20/ty-article/nso-ghana-op-exposed-never-before-seen-pegasus-spyware-footage-workers-passports/0000017f-f1fb-df98-a5ff-f3ffb9a20000 (last accessed June 5, 2023).

[41] *Id.* ("'I coached them on how to use it,' one employee told 'Hamakor.'")

[42] U.S. Dep't of State, Bureau of Democracy, H.R. and Lab., 2016 Country Reports on Human Rights Practices: Ghana, 2016. *Available at:* https://www.state.gov/wp-content/uploads/2019/01/Ghana-1.pdf

[43] *Id.*

of the conservative Saudi ruling entities.[44] Jamal eventually was reappointed as Editor of *Al-Watan*, but was once again fired after three years for writing articles related to the rights of women and abuses of power perpetrated by the Saudi religious police.[45] These pieces were deemed "offensive" by Saudi authorities.[46]

88. Public discourse in Saudi Arabia is tightly controlled by the monarchy, and the news outlets for which Jamal worked were no exception. The ruling royal family in Saudi Arabia, the al-Sauds, are legitimized and supported by a council of fundamentalist Islamic religious leaders called the *ulama*, who adhere to what is commonly called the "Wahhabi" school of Islamic jurisprudence.

89. Jamal covered the Soviet-Afghan War, and, like many Muslims the world over, was initially supportive of the resistance to the Soviet invasion.

90. However, Jamal staunchly opposed the violence perpetuated by Osama bin Laden that grew out of the Soviet-Afghan War, and reportedly urged bin Laden to abandon *jihad* on more than one occasion during the 1990s.

91. An avowed anti-extremist, Jamal refused to be associated with the growing radical movement and embraced the western idea of the separation of church and state, further angering the *ulama* in Saudi Arabia.

[44] After an Al Qaeda bombing that killed twenty-five in Riyadh, Saudi Arabia, Jamal criticized the Saudi religious establishment directly, saying those "who instigated or justified the attacks" would also "have a painful impact on the peaceful nature of our nation." *See* Ben Hubbard, *MBS: The Rise to Power of Mohammed Bin Salman* 75 (2020).

[45] Justin D. Martin, "Sidelined Speech in Saudi Arabia," May 21, 2010, https://archives.cjr.org/behind_the_news/sidelined_speech_in_saudi_arab.php (last accessed June 5, 2023).

[46] One such article asked the reader to imagine the chaos that would be caused by a girl riding a camel to university, a critique of Saudi Arabia's ban on women driving. Ben Hubbard, *MBS: The Rise to Power of Mohammed Bin Salman* 75-76 (2020).

92. As a result, Jamal was forced out of his job as editor at Al-Watan in 2003, saying "The clergy. They didn't like me. They didn't like the way I ran the paper." Ever hopeful, Jamal also stated of his country, "I see change, and I would like to be part of that change."[47]

93. Jamal's beliefs and advocacy never faltered. When he covered the Arab Spring,[48] Jamal was hopeful that Saudi Arabia would listen to the people and embrace change. Jamal criticized the violent response to the protests, saying "confronting—rather than acceding to—the demands for change [embodied in the Arab Spring] is what led to the current chaos in the region."[49]

94. Just as the Arab Spring movement was getting started, Jamal and Hanan met at a conference in the UAE in 2009, and instantly connected. Hanan described meeting him like finding her "twin." Jamal was married at the time, but the two kept in touch as friends over the next eight years, often exchanging messages and sharing their viewpoints on politics and a hope for peace and democracy in the Middle East.

95. Throughout his career, Jamal wrote thought-provoking articles concerning equal rights for women and minorities, religious freedom, and other issues challenging the status quo in the Middle East, and in Saudi Arabia in particular. In 2016, Hanan and Jamal were constantly in touch regarding various global political matters, including the election of Donald J. Trump to the United States Presidency. Jamal shared his misgivings with Hanan, then in late 2016, publicly shared his concerns by delivering a speech critical of the election of President Trump at the Washington Institute for Near East Policy. This criticism angered the ruling Saudis, who were working to foster a friendly relationship with Trump, and Jamal was subsequently placed under

[47] Peter Bergen, "Jamal Khashoggi was a journalist, not a jihadist," October 22, 2018, https://edition.cnn.com/2018/10/22/opinions/khashoggi-was-journalist-not-jihadist-bergen/index.html (last accessed June 5, 2023).

[48] The "Arab Spring" was a series of anti-Government protests emerging in Tunisia in 2010, and spreading to, among other places, Egypt, Libya, Saudi Arabia, Yemen, and Bahrain.

[49] "Khashoggi: resistance to Arab Spring caused chaos and I wish Saudi Arabia would have embraced it," *MEMO*, *Middle East Monitor*, August 31, 2017, https://www.middleeastmonitor.com/20170831-khashoggi-resistance-to-arab-spring-caused-chaos-and-i-wish-saudi-arabia-would-have-embraced-it/ (last accessed June 5, 2023).

house arrest. During this time, Hanan remained in touch with Jamal, supporting him and assuaging him during his confinement. Hanan communicated with journalists around the world in an attempt to support Jamal and draw attention to his plight.

96. In June 2017, the Saudi government lifted Jamal's house arrest and allowed him to travel to the UAE to attend a conference. Upon arrival at the Abu Dhabi airport, he was denied entry and flew back to Saudi Arabia. This action tipped him off that he was in growing danger, and as a result, Jamal made the difficult decision to flee Saudi Arabia, seeking refuge in the United States. Once Jamal arrived in the U.S., he invited Hanan to visit and reconnect with him in person in Virginia. Shortly after his arrival, Jamal became a contributor to the Washington Post.

97. Jamal's outspoken statements that landed him in dangerous waters in 2016 and 2017 came amid a larger crackdown on free speech in Saudi Arabia. In Jamal's own words,

> Dozens of Saudi intellectuals, clerics, journalists, and social media stars have been arrested in the past 2 months—the majority of whom, at worst, are mildly critical of the government. . . . How can we become more moderate when such extremist views are tolerated? How can we progress as a nation when those offering constructive feedback and (often humorous) dissent are banished?[50]

98. On September 18, 2017, Khashoggi's first column for *The Washington Post* appeared with a stark opening line: "When I speak of the fear, intimidation, arrests and public shaming of intellectuals and religious leaders who dare to speak their minds, and then I tell you that I'm from Saudi Arabia, are you surprised?"[51]

99. Jamal continued to bravely speak out against the manner in which Saudi Arabia was being ruled, writing in a November 15, 2017 opinion in *The Washington Post* that he

[50] Jamal Khashoggi, "Saudi Arabia's crown prince wants to 'crush extremists.' But he's punishing the wrong people," *The Washington Post*, October 31, 2017, https://www.washingtonpost.com/news/global-opinions/wp/2018/10/06/read-jamal-khashoggis-columns-for-the-washington-post/ (last accessed June 5, 2023).

[51] Jamal Khashoggi, "Saudi Arabia wasn't always this repressive. Now it's unbearable," *The Washington Post*, September 18, 2017, https://www.washingtonpost.com/news/global-opinions/wp/2017/09/18/saudi-arabia-wasnt-always-this-repressive-now-its-unbearable/ (last accessed June 5, 2023).

"champion[s] a real campaign to tackle the rampant corruption that is draining Saudi resources."[52] This opinion in particular focused on Crown Prince Mohammed bin Salman ("MBS")—explicitly stating that he was "acting like Putin" by "imposing very selective justice" in his "crackdown on even the most constructive criticism."[53]

100. It was during this same time period that Jamal and Hanan's longtime friendship evolved into romance, and Hanan encouraged Jamal to "make use of his freedom" after fleeing Saudi Arabia. The two continued to bond over shared political beliefs, and often discussed the fraught state of much of the Middle East. Jamal confided in Hanan that he did not consider himself a "dissident," but rather he had a profound love for Saudi Arabia, and for that reason, he felt he must keep writing and raising his voice to effect change there. Jamal told Hanan he was lonely in the United States, and he longed to be able to return to his home.

101. Upon information and belief, in November 2017, the first Pegasus attempts were made on one of Hanan's cell phones, just as she was growing closer with Jamal. These were ESEM text messages that were personalized to induce her to follow the malicious link containing Pegasus.

102. In one instance, at 06:46:59 GMT on November 26, 2017, Hanan received a text message stating that a flower bouquet was sent to her. She later clicked and followed the link and was rerouted to a disabled Pegasus link. Citizen Lab attributed the domain name in these links to an agency of the UAE.

103. At least five more attempts were made via ESEM text messages sent to Hanan's phone in November 2017.

[52] Jamal Khashoggi, "Saudi Arabia's crown prince is acting like Putin," *The Washington Post*, November 5, 2017, https://www.washingtonpost.com/news/global-opinions/wp/2017/11/05/saudi-arabias-crown-prince-is-acting-like-putin/ (last accessed June 5, 2023).

[53] *Id.*

104. Jamal and Hanan continued their relationship, and in April 2018, Jamal proposed to Hanan and gave her an engagement ring. He later also bought her a wedding ring in Tysons Corner, Virginia.

105. Upon information and belief, in April 2018, more malicious text messages using Pegasus spyware were sent to Plaintiff's phone.

106. In April 2018, while working as a flight attendant, Hanan arrived at the Dubai International Airport and found seven Emirati intelligence officers waiting for her. Hanan was blindfolded, handcuffed, and transported to a remote interrogation cell where she was questioned about Jamal and his activities for over 17 hours. Hanan was detained and her captors took both of her cell phones that she had been using to communicate with Jamal. Citizen Lab later confirmed in its analysis that it was likely during this time that Pegasus was manually installed onto at least one of her phones. NSO Group touts the ability for Pegasus to be installed through multiple mechanisms, and physical installation is advertised explicitly by NSO Group.[54]

107. Hanan was placed under house arrest in the UAE until May 2018, when she returned to the United States to be with Jamal. In her long tenure as a flight attendant, with many trips into and out of the UAE, Hanan had never been detained or questioned by the authorities before becoming engaged to Jamal. Hanan later stated that she feared for her life, and it was apparent to her immediately that she was being held because of her relationship to Jamal. She was never charged with a crime, nor offered any justification for her imprisonment.

108. Unbeknownst to Hanan, upon information and belief, the Kingdom of Saudi Arabia had leveraged its relationship with a key ally, the United Arab Emirates, to install Pegasus on her phones, which would then allow MBS to monitor and track Jamal.[55]

[54] 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, 2017, https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/; *see also* Exhibit 1 at 13.

[55] This is not the first time that the UAE has acted at the behest of Saudi Arabia to silence critics of the Kingdom. In 2018, security officers in the UAE pulled over Saudi women's rights activist

109. Once Hanan arrived back in the United States, Jamal warned her that it would not be easy for her to be with him, and again asked if she truly wanted to spend her life with him. For Hanan, it was no question —"yes." Unbeknownst to either of the two at the time, the depth of their relationship would put them both in danger through the now-constant avenue Defendants and their clients had into their everyday lives, communications, and intimate conversations.

110. On June 2, 2018, Hanan and Jamal were married according to Islamic tradition by Imam Anwar Hajjaj of the Open University in Alexandria, VA, which was observed and attended by two witnesses. However, due to the level of threat Jamal was under, and the recent experience Hanan endured in the UAE, the two kept their relationship, and marriage, very quiet, alerting only select family members and friends. They spent the next weeks moving into and decorating their shared apartment in Virginia and making it their home.

111. Although Hanan's job as a flight attendant kept her traveling often, anytime she was able to be, she was home with Jamal. When the two were forced to be apart, they were in frequent contact through text messages, WhatsApp, phone calls, and various other apps Jamal insisted they use for privacy. Unfortunately, Jamal's suspicions were well-founded, but use of multiple apps or frequently changing SIM cards was no match for NSO Group's technology. Neither suspected that Hanan herself might become a target.

112. During this time, Jamal continued to stoke the ire of MBS, writing that MBS was "punishing the wrong people."[56] After MBS rounded up and detained a number of "intellectuals

Loujain al-Hathloul in Abu Dhabi and deported her to Saudi Arabia. Loujain al-Hathloul has also been surveilled using the Pegasus spyware. *See* U.S. Dep't of State, Bureau of Democracy, H.R. and Lab., 2018 Country Reports on Human Rights Practices: United Arab Emirates, 2018. *Available at:* https://www.state.gov/wp-content/uploads/2019/03/UNITED-ARAB-EMIRATES-2018.pdf at 11; Joel Schectman and Christopher Bing, "How a Saudi woman's iPhone revealed hacking around the world," *Reuters*, February 17, 2022, https://www.reuters.com/technology/how-saudi-womans-iphone-revealed-hacking-around-world-2022-02-17/ (regarding the UAE surveilling al-Hathloul with Pegasus) (last accessed June 5, 2023).

[56] Jamal Khashoggi, "Saudi Arabia's crown prince wants to 'crush extremists.' But he's punishing the wrong people," *The Washington Post*, October 31, 2017,

and religious leaders who dare to express opinions," contrary to his own safety, Jamal wrote "…I am raising my voice. To do otherwise would betray those who languish in prison. I can speak when so many cannot."[57] Hanan continued to support him, encouraging him to use his freedom in the United States to speak out.

113. Upon information and belief, during this time, MBS became increasingly obsessed with Jamal. Upon information and belief, all of Jamal and Hanan's conversations—by phone, message, or in person—were available to NSO Group and ultimately relayed to the Saudis, via the UAE, providing key information and proof of Jamal's persistent belief that Saudi Arabia needed reform.

114. On September 6-7, 2018, Jamal and Hanan spent what would be their last days together in a hotel in New York City. Hanan knew that Jamal was planning to go to Turkey and Jamal shared with Hanan his full travel plans, including his planned return that tragically never occurred. They discussed their future together, including having property both in Turkey and in Virginia, keeping their Tysons Corner home.

115. The two remained in contact by phone while Jamal was traveling. Their last communications occurred on September 30, 2018, a message Hanan did not receive until October 1, 2018, only 24 hours before Jamal's death. That last communication from Jamal to Hanan wished her a happy birthday.

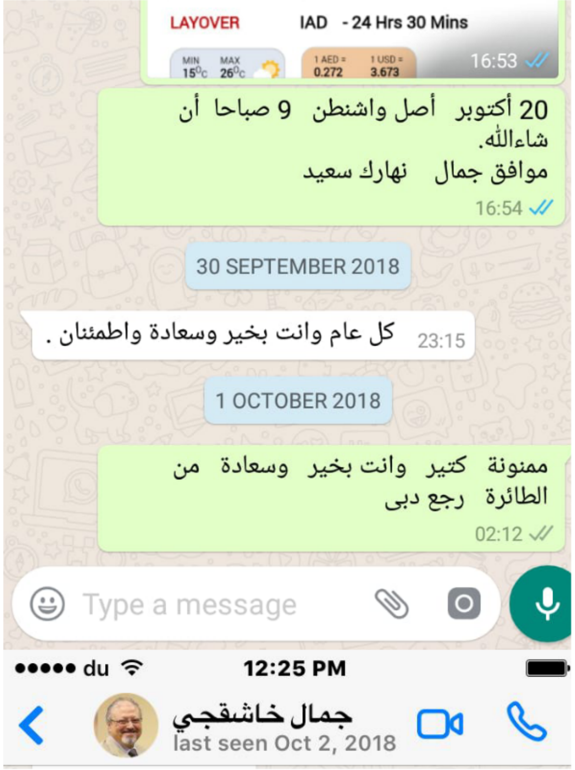
116. Translated from Arabic to English, their last messages state:

> *Hanan*: On October 20, 2018 I will arrive in Washington at 9 am. Good Luck Jamal Have a good Day
>
> *Jamal*: (September 30) Happy Birthday, with happiness and peacefulness

https://www.washingtonpost.com/news/global-opinions/wp/2018/10/06/read-jamal-khashoggis-columns-for-the-washington-post/ (last accessed June 5, 2023).

[57] Jamal Khashoggi, "Saudi Arabia wasn't always this repressive. Now it's unbearable," *The Washington Post*, September 18, 2017, https://www.washingtonpost.com/news/global-opinions/wp/2017/09/18/saudi-arabia-wasnt-always-this-repressive-now-its-unbearable/ (last accessed June 5, 2023).

> *Hanan*: (October 1) thank You I hope you are fine and happy. I am in the aircraft headed to Dubai[58]



20 أكتوبر أصل واشنطن 9 صباحا أن شاءالله.
موافق جمال نهارك سعيد
16:54

30 SEPTEMBER 2018

كل عام وانت بخير وسعادة واطمئنان .
23:15

1 OCTOBER 2018

ممنونة كتير وانت بخير وسعادة من الطائرة رجع دبى
02:12

117. On October 2, 2018, Jamal Khashoggi disappeared after visiting the Saudi consulate in Istanbul.

118. Back home, Hanan was shocked and terrified. Her worst fears were becoming reality—and being broadcast on a global stage. As the days and weeks passed, it became apparent that Jamal had been assassinated. Hanan watched in indescribable grief and growing fear for her own safety.

119. The details of Jamal's death were well-documented and publicized by nearly every major news outlet in the world. Hanan was forced to relive the grisly death and dismemberment of her husband time and time again.

[58] Screenshot provided courtesy of Hanan Khashoggi.

120. The CIA ultimately concluded that Saudi Arabia's Crown Prince Muhammad bin Salman orchestrated and approved of the operation to kill Jamal, and members of MBS's personal security team made up the 15-member hit squad.

121. The CIA's assessment aligned with what much of the general public already knew: "[t]he Crown Prince viewed Khashoggi as a threat to the Kingdom and broadly supported using violent measures if necessary to silence him."[59]

122. Regarding Jamal Khashoggi, NSO Group has publicly maintained that it had "nothing to do with this horrible murder," despite significant evidence to the contrary.[60]

123. Upon information and belief, Defendants and their clients were aware that Jamal and Hanan were living together in Virginia and that Hanan has continued to reside in Virginia, where she was monitored for—at least—a year through NSO Group's product on her devices.

THE NSO GROUP REVEALED

124. In July of 2021, multiple media outlets partnered with "Forbidden Stories," on the "Pegasus Project." [61] The group consisted of a network of journalists with a mission to "protect, pursue and publish the work of other journalists facing threats, prison, or murder" to expose NSO Group's technology and use of that spyware on journalists and activists around the world.[62]

[59] U.S. Office of the Director of National Intelligence, Assessing the Saudi Government's Role in the Killing of Jamal Khashoggi, February 11, 2021. *Available at:* https://www.dni.gov/files/ODNI/documents/assessments/Assessment-Saudi-Gov-Role-in-JK-Death-20210226v2.pdf.

[60] Stephanie Kirchgaessner, "Saudis behind NSO spyware attack on Jamal Khashoggi's family, leak suggests," *The Guardian*, July 18, 2021, https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus#:~:text=The%20phone%20analysis%20discoveries%20and,Turkish%20inquiry%20into%20his%20murder (last accessed June 5, 2023).

[61] The Pegasus Project media partners: The Guardian, Le Monde, The Washington Post, Süddeutsche Zeitung, Die Zeit, Aristegui Noticias, Radio France, Proceso, OCCRP, Knack, Le Soir, Haaretz/TheMarker, The Wire, Daraj, Direkt36, PBS Frontline.

[62] "About the Pegasus Project," https://forbiddenstories.org/about-the-pegasus-project/. (last accessed June 6, 2023).

125. Around this time, Hanan was approached by a journalist from the Washington Post to inform her that analysis from Amnesty International showed evidence that Hanan's phones may have been infiltrated. Further, more in-depth analysis performed by Citizen Lab confirmed that suspicion in November of 2021.

126. Defendants have been the subject of significant media and political attention for several years. In addition to being placed on the U.S. Department of Commerce's "Entity List," NSO Group and Q Cyber have been named as Defendants in several pending cases in the United States and internationally. The facts of those cases have significant overlap with Hanan's claims in this present action. In the United States, Plaintiffs Apple and WhatsApp (Meta) have filed suit against NSO Group for alleged infiltrations of their servers, impacting thousands of Apple and WhatsApp users. WhatsApp has successfully proceeded past the motion to dismiss phase and all other matters are currently pending.[63] In *Dada v. NSO Group Technologies Limited*, a consortium of journalists from El Salvador working for the news publication *El Faro* have brought suit against NSO Group and Q Cyber for the targeting, infiltration, and breaches of privacy of their own devices. Much like Hanan's case, the Plaintiffs in *Dada* were allegedly targeted as a result of their perceived threat to the Salvadoran government.[64]

NSO GROUP'S HARMS TO HANAN KHASHOGGI CONTINUE

127. As a result of being targeted by NSO Group and its client(s), Hanan's life has been irrevocably altered.

128. Not only has Hanan suffered the unimaginable loss of her husband, she has also had to rearrange her life to adjust to the reality of being a target of dangerous, violent, and powerful authoritarian actors, including the loss of her career and livelihood.

[63] *WhatsApp Inc. v. NSO Grp. Techs. Ltd.*, 17 F.4th 930 (9th Cir. 2021), *cert. denied*, 214 L. Ed. 2d 333, 143 S. Ct. 562 (2023).

[64] Amended Compl., *Dada v. NSO Group Technologies*, 3:22-cv-07513-WHA (N.D. Cal. December 16, 2022), ECF No. 31.

129. Defendants violated Hanan's privacy in one of the most pervasive fashions imaginable. All of her messages, app activity, emails, financial information, medical information, and more were available to Defendants, and upon information and belief, made available to Defendants' clients. Additionally, Hanan's private conversations in the intimacy of her own home and marriage were invaded by agents of an authoritarian government that, upon information and belief, ultimately used that information to murder her husband. Hanan was violated in a way few others could even fathom—NSO Group laid every intimate detail of her life bare.

130. Hanan was forced to leave her job of over 20 years due to the harassment and intimidation she suffered from alleged client(s) of NSO Group. Even after Jamal's death, Hanan continued to be targeted for her relationship with him. Hanan eventually lost her career as a flight attendant due to the risks to her safety and the time she (involuntarily) spent away from work. Several months after Jamal was murdered, in February 2019, Hanan was again confronted by UAE officials and again detained and placed under house arrest, this time for more than two months. When the time came for Hanan's contract to be renewed with Emirate Airlines, her boss told her they were letting her go.

131. Due to the physical risks of travel, and fear for her family's safety, Hanan has been unable to see her family in the Middle East for several years.

132. Hanan is still suffering from the effects of the NSO Group infiltration of her devices today. She lives in a state of constant hyper-vigilance, unable to safely participate in social activities, constantly looking over her shoulder.

133. As a result of the intimidation and threat of danger to Hanan's life, she is currently seeking the legal protection of political asylum in the United States.

V. CAUSES OF ACTION

COUNT 1: VIOLATIONS OF THE COMPUTER FRAUD AND ABUSE ACT 18 U.S.C. § 1030 *et seq.*

134. Plaintiff realleges and incorporates by reference each preceding and succeeding paragraph as though set forth fully at length herein.

135. As detailed in this pleading, between November 8, 2017 and July 10, 2018, Defendants accessed or attempted to access Plaintiff's devices on multiple occasions, without authorization. Plaintiff owned the affected devices, and those devices contained a plethora of private information, including personal communications, photographs, and videos.

136. Pursuant to the Computer Fraud and Abuse Act ("CFAA"), the intentional access of a computer without authorization, or in excess of authorized access, to obtain information from any protected computer is prohibited. 18 U.S.C. § 1030(a)(2)(C).

137. The devices storing Plaintiff's data and personal information are "protected computers" because they are used in or affected interstate commerce or communications. 18 U.S.C. § 1030(e)(2).

138. Defendants violated 18 U.S.C. § 1030(a)(2)(C) by intentionally accessing and/or causing to be accessed Plaintiff's devices without authorization and obtaining information from those devices.

139. Defendants accessed and/or caused to be accessed Plaintiff's devices without authorization through attacks that enabled the surreptitious installation of Pegasus on Plaintiff's devices.

140. Defendants infiltrated Plaintiff's devices with Pegasus to enable real-time surveillance of Plaintiff and her husband, including through unauthorized use of the device's microphone and camera, and to exfiltrate private data from those devices to Defendants and their clients. Once installed, Pegasus provided Defendants and their clients with nearly unfettered access to Plaintiff's devices.

141. Although by its very nature and design, Pegasus leaves very little trace, if any, of its presence on a device, forensic investigation completed by Citizen Lab on December 20, 2021 confirmed the presence of Pegasus and NSO Group-related infiltration evidence on Plaintiff's devices. Upon information and belief, Defendants and their clients obtained both stored and real-time data and surveillance from Plaintiff's targeted devices.

142. A private right of action exists for any person who suffers damage or loss by reason of a violation of the CFAA, provided that one of the statutorily enumerated factors are present. 18 U.S.C. §1030(g).

143. Plaintiff suffered both damage and loss as a result of the infiltration of her devices by NSO Group and its clients.

144. Among the factors enumerated for civil recovery are: "(I) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value. . . (III) physical injury to any person; [and] (IV) a threat to public health or safety. 18 U.S.C. § 1030(c)(4)(A)(i)(I, III-IV).

145. Plaintiff's total economic loss stemming from the Pegasus attacks exceeded $5,000 in aggregate during a one-year period, including, but not limited to, the costs of fleeing to the United States, the loss of her and her husband's income, and the costs of replacing her devices.

146. There is no economic loss requirement for factors (III) and (IV) listed above, although Plaintiff has experienced significant damage and loss falling into those categories.

147. Plaintiff experienced the suffering, both physical and mental, of being held and interrogated by UAE officials (who, upon information and belief, used that time to physically install Pegasus on Plaintiff's devices) resulting in physical injury to Plaintiff.

148. Jamal Khashoggi was also physically injured as a result of Defendants' violations of the CFAA. Defendants contributed to Jamal's death by knowingly providing Pegasus and other products to clients with known human rights violations, by aiding them and providing support to those clients, and by intentionally, recklessly, and/or negligently aiding and abetting in the commission of the crimes of torture and murder.

149. Defendants further contributed to a threat to public health or safety by perpetuating their client(s)' crimes and human rights violations.

150. Defendants violated 18 U.S.C. § 1030(b) by conspiring and attempting to commit the violations alleged in the preceding paragraphs.

151. In the alternative, Defendants knowingly and intentionally aided and abetted their clients in the violations of 18 U.S.C. § 1030 alleged in the preceding paragraphs.

COUNT 2: VIOLATIONS OF THE VIRGINIA COMPUTER CRIMES ACT Va. Code § 18.2-152.1 *et seq.*

152. Plaintiff realleges and incorporates by reference each preceding and succeeding paragraph as though set forth fully at length herein.

153. Pursuant to the Virginia Computer Crimes Act ("VCCA"), Va. Code § 18.2-152.1 *et seq*., any person whose property or person is injured by a provision of the Act "may sue therefor and recover any damages sustained and the costs of the suit." Va. Code § 18.2-152.12(A).

154. The VCCA further states that it is unlawful to "[i]nstall or cause to be installed, or collect information through, computer software that records all or a majority of the keystrokes made on the computer of another." Va. Code § 18.2-152.4 (A)(8).

155. As alleged in the preceding paragraphs, Defendants accessed Plaintiff's devices and personal information without authorization, in violation of the VCCA. Defendants and their clients knew that Hanan and Jamal were living in Virginia at the time Pegasus was installed on Plaintiff's devices. Defendants installed, or caused to be installed, Pegasus on Plaintiff's devices.

156. Defendants and their clients used false pretenses to commit larceny regarding private messages, emails, conversations, location information, and other personal information of both Plaintiff and her husband.

157. Upon information and belief, Defendants and their clients used false pretenses by sending ESEM messages to Plaintiff's devices in order to entice her to engage with the links thus activating Pegasus on her devices.

158. Defendants then used the personal information gleaned from this infiltration to cause substantial harm to Plaintiff, as enumerated in the preceding paragraphs.

159. Defendants further violated Va. Code § 18.2-152.4, under which it is unlawful to "remove [] or otherwise disable any computer data . . . from a computer. . . ." It is also unlawful for a person to use a computer to "make . . . an unauthorized copy, in any form, . . . of computer data."

160. As alleged in the preceding paragraphs, Defendants also violated the VCCA through their actions in illegally accessing and misappropriating Plaintiff's personal data.

161. Plaintiff has sustained substantial damages and costs, as alleged herein, related to investigating and responding to Defendants' offenses, severe mental anguish and emotional distress, the physical injury to herself and her husband, and the resulting loss of her husband, loss of her income and job, and other consequential damages.

162. Evidence of consequential damages falls within the "any damages" language of the VCCA. *A.V. ex rel Vanderhye*, 562 F.3d 630, 647 (4th Cir. 2009).

163. Pursuant to Va. Code § 18.2-152.3, Plaintiff is also entitled to recover the costs of this suit.

COUNT 3:
NEGLIGENCE

164. Plaintiff realleges and incorporates by reference each preceding and succeeding paragraph as though set forth fully at length herein.

165. At all relevant times, Defendants developed, set up, maintained, marketed, advertised, controlled, and sold their spyware infrastructure to nation-state clients.

166. Defendants owed Plaintiff a duty to exercise reasonable care in the development, set up, maintenance, operation, marketing, advertisement, control, and sale of its spyware infrastructure to not create an unreasonable risk of harm from the use of its infrastructure and to protect Plaintiff from unreasonable risk of injury from and in the use of its spyware infrastructure.

167. Imposing a duty on Defendants is not burdensome and would benefit the community of journalists, activists, dissidents, and their family members and loved ones, at large.

168. Plaintiff was a foreseeable victim of the Defendants' spyware infrastructure. Defendants sought out, marketed, and sold its spyware infrastructure to countries with disturbing human rights records.

169. As a result of Defendants' failure to exercise reasonable care when they repeatedly sold Pegasus to clients that were widely known to violate human rights and do harm to dissenters, Defendants caused and proximately caused harm to Plaintiff.

170. Defendants have breached their duties of care owed to Plaintiff through their affirmative malfeasance, actions, business decisions, and policies in the development, setup, management, maintenance, operation, marketing, advertising, promotion, supervision, and control, and sale of its spyware infrastructure.

171. As a direct and proximate result of Defendants' breach of one or more of their duties, Plaintiff was harmed. Specifically, Defendants breached their duty by knowingly marketing and selling their spyware to countries with long histories of human rights abuses.

172. Defendants' breach of one or more of their duties was a substantial factor in causing harms and injuries to the Plaintiff.

173. Defendants' conduct, as described above, was intentional, fraudulent, willful, wanton, reckless, malicious, fraudulent, oppressive, extreme, and outrageous, and displayed an entire want of care and a conscious and depraved indifference to the consequences of their conduct, including to the health, safety, and welfare of the likely targets of their clients, and warrants an award of punitive damages in an amount sufficient to punish the Defendants and deter others from like conduct.

174. Plaintiff demands judgment against Defendants for injunctive relief as described below, and for compensatory, treble, and punitive damages, together with interest, costs of suit, attorneys' fees, and all such other relief as the Court deems proper.

COUNT 4: TRESPASS TO CHATTELS

175. Plaintiff realleges and incorporates by reference each preceding and succeeding paragraph as though set forth fully at length herein.

176. At all times mentioned in this Complaint, Plaintiff had legal title to and actual possession of her cell phones, except where explicitly indicated.

177. Plaintiff owned two cell phone devices targeted in the Pegasus attack in which she had a possessory interest in and the exclusive right to use the targeted devices. These devices contained Plaintiff's private information, including phone calls, text messages and other communications.

178. Defendants intentionally intermeddled with Plaintiff's phones/devices when they gained access to Plaintiff's devices by use of their proprietary "Pegasus" spyware which allowed all information on Plaintiff's phone to be downloaded and provided to Defendant's clients.

179. The technology used allowed Defendants and their clients to review in real time any phone call, text, or other communication, GPS activity, as well as turn Plaintiff's phones into a remote listening device by surreptitiously activating her microphone and camera at any time. The value of the devices was thus impaired for Plaintiff's use, becoming effectively valueless to Plaintiff.

COUNT 5: INTENTIONAL INFLICTION OF EMOTIONAL DISTRESS

180. Plaintiff realleges and incorporates by reference each preceding and succeeding paragraph as though set forth fully at length herein.

181. Defendants acted negligently as detailed above.

182. Defendants' conduct was intentional and malicious and done for the purpose of causing Plaintiff to suffer humiliation, mental anguish, and emotional and physical distress.

183. Plaintiff suffered severe emotional distress and the Plaintiff's severe emotional distress was proximately caused by the Defendants' conduct.

184. Plaintiff continues to suffer from fear, anxiety, and extreme stress as a result of having both of her phones hacked and turned into continuously operating spy devices.

185. As a further proximate result of Defendants' actions and the consequences proximately caused by them, as alleged above, Plaintiff suffered severe humiliation, mental anguish, and emotional and physical distress, resulting in damages.

COUNT 6: NEGLIGENT INFLICTION OF EMOTIONAL DISTRESS

186. Plaintiff realleges and incorporates by reference each preceding and succeeding paragraph as though set forth fully at length herein.

187. Defendants acted negligently as detailed above.

188. Defendants knew, or should have known, that failure to exercise due care in the selling of their spyware infrastructure would cause Plaintiff severe emotional distress.

189. As a further proximate result of Defendants' actions and the consequences proximately caused by them, as alleged above, Plaintiff suffered severe emotional distress and mental suffering, resulting in damages.

COUNT 7: EQUITABLE RELIEF

190. Plaintiff realleges and incorporates by reference each preceding and succeeding paragraph as though set forth fully at length herein.

191. Plaintiff demands the identities of Defendants' clients and any of their agents that targeted and accessed her devices.

192. Plaintiff demands disclosure of all contracting documents between Defendants and their clients that targeted and accessed her devices.

193. Defendants publicly claim that they can monitor and forbid any misuse of their spyware infrastructure. As such, Plaintiff demands permanent cessation, in the form of an injunction, of all monitoring of her personal electronic devices.

VI. PRAYER FOR RELIEF

Plaintiff demands judgment against Defendants to the full extent of the law, including but not limited to:

1. Judgment for Plaintiff and against Defendants on all Counts enumerated herein;
2. damages (both past and future) to compensate Plaintiff for injuries sustained as a result of Defendants' conduct, including but not limited to physical pain and suffering, mental anguish, loss of enjoyment of life, emotional distress, expenses for hospitalizations and medical treatments other economic harm that includes but is not limited to lost earnings and loss of earning capacity;
3. damages to compensate Plaintiff for loss of consortium, companionship, services, society, love, and comforts, and alteration their martial association, and mental anguish and emotional distress;
4. exemplary, treble, and/or punitive damages in an amount in excess of the jurisdictional limits;
5. attorneys' fees;
6. experts' fees;
7. costs of litigation;
8. pre-judgment and post-judgment interest at the lawful rate;
9. injunctive relief, including, but not limited to, ordering Defendants to stop the harmful conduct alleged herein,
10. any other relief as this Court may deem equitable and just, or that may be available.

VI. JURY DEMAND

Plaintiff demands a trial by jury on all issues so triable.

Dated: June 16, 2023

Respectfully submitted,

MICHAEL PENDELL (*pro hac vice forthcoming*)
MOTLEY RICE LLC
One Corporate Center
20 Church S., 17TH Floor
Hartford, CT 06103
T: 860.882.1681
mpendell@motleyrice.com

ANNIE E. KOUBA (*pro hac vice forthcoming*)
ROSS HEYL (*pro hac vice forthcoming*)
MOTLEY RICE LLC
28 Bridgeside Blvd
Mt. Pleasant, SC 29464
T: 843.216.9000
akouba@motleyrice.com
rheyl@motleyrice.com

RANDA FAHMY (*pro hac vice forthcoming*)
282 35th Street
Avalon, NJ 08202
T: 202.352.2186
Randa@fahmyhudome.com

/s/ Steven T. Webster
Steven T. Webster (VSB No. 31975)
swebster@websterbook.com
Aaron S. Book (VSB No. 43868)
abook@websterbook.com
Webster Book LLP
300 N. Washington St., Suite 404
Alexandria, Virginia 22314
(888) 987-9991 (telephone and fax)

EXHIBIT
1

Pegasus – Product Description

Contents

List of Tables

List of Figures

Introduction

Pegasus is a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device. This breakthrough solution was developed by veterans of elite intelligence agencies to provide governments with a way to address the new communications interception challenges in today's highly dynamic cyber battlefield. By capturing new types of information from mobile devices, Pegasus bridges a substantial technology gap to deliver the most accurate and complete intelligence for your security operations.

Overcoming Smartphone Interception Challenge

The rapidly growing and highly dynamic mobile communications market - characterized by the introduction of new devices, operating systems and applications on virtually a daily basis – requires a rethinking of the traditional intelligence paradigm. These changes in the communications landscape pose real challenges and obstacles that must be overcome by intelligence organizations and law enforcement agencies worldwide:

- Encryption: Extensive use of encrypted devices and applications to convey messages
- Abundance of communication applications: Chaotic market of sophisticated applications, most of which are IP-based and use proprietary protocols
- Target outside interception domain: Targets' communications are often outside the organization's interception domain or otherwise inaccessible (e.g., targets are roaming, face-to-face meetings, use of private networks, etc.)
- Masking: Use of various virtual identities which are almost impossible to track and trace
- SIM replacement: Frequent replacement of SIM cards to avoid any kind of interception
- Data extraction: Most of the information is not sent over the network or shared with other parties and is only available on the end-user device
- Complex and expensive implementation: As communications become increasingly complex, more network interfaces are needed. Setting up these interfaces with service providers is a lengthy and expensive process, and requires regulation and standardization

Standard Interception Solutions Are Not Enough

Until the above mentioned challenges are addressed and resolved, criminal and terrorist targets are likely "safe" from standard and legacy interception systems, meaning that valuable intelligence is being lost. These standard solutions (described in the sections below) deliver only partial intelligence, leaving the organizations with substantial intelligence gaps.

Passive Interception

Passive interception requires very deep and tight relationships with local service providers (cellular, Internet and PSTN providers) and traditionally has allowed for proper monitoring of text messages and voice calls. However, most contemporary communications is comprised of IP-based traffic, which is extremely difficult to monitor with passive interception due to its use of encryption and proprietary protocols.

Even when this traffic is intercepted, it typically carries massive amounts of technical data that is not related to the actual content and metadata being communicated. Not only does this result in frustrated analysts and wasted time wading through irrelevant data, it also provides a partial snapshot (at best) of the target's communications. In addition, the number of interfaces required to cover the relevant service providers broadens the circle of entities exposed to sensitive information and increases the chance of leakage.

Tactical GSM Interception

Tactical GSM interception solutions effectively monitor voice calls and text messages in GSM networks. When advanced cellular technologies are deployed (3G and LTE networks), these solutions become less efficient. In such cases, it is required to violently downgrade the target to a GSM-based network, which noticeably impacts the user experience and functionality.

These solutions also require a well-trained field tactical team located near the monitored target. Thus, in the majority of cases where the target location is unknown, these solutions become irrelevant. In other cases, placing a tactical team close to the target may pose serious risk both to the team and to the entire intelligence operation.

Malicious Software (Malware)

Malware presumably provides access to the target's mobile device. However, it is not completely transparent and requires the target's involvement to be installed on their devices. This type of engagement usually takes the form of multiple confirmations and approvals before the malware is functional. Most targets are unlikely to be fooled into cooperating with malware due to their high level of sensitivity for privacy in their communications.

In addition, such malware is likely to be vulnerable to most commercially available anti-virus and anti-spyware software. As such, they leave traces and are fairly easily detected on the device.

Cyber Intelligence for the Mobile World

Pegasus is a world-leading cyber intelligence solution that enables law enforcement and intelligence agencies to remotely and covertly extract valuable intelligence from virtually any mobile device. This breakthrough solution was developed by veterans of elite intelligence agencies to provide governments with a way to address the new communications interception challenges in today's highly dynamic cyber battlefield.

By capturing new types of information from mobile devices, Pegasus bridges a substantial technology gap to deliver the most accurate and complete intelligence for your security operations. This solution is able to penetrate the market's most popular smartphones based on BlackBerry, Android, iOS and Symbian operating systems.

Pegasus silently deploys invisible software ("agent") on the target device. This agent then extracts and securely transmits the collected data for analysis. Installation is performed remotely (over-the-air), does not require any action from or engagement with the target, and leaves no traces whatsoever on the device.

Benefits of Pegasus

Organizations that deploy Pegasus are able to overcome the challenges mentioned above to achieve unmatched mobile intelligence collection:

- Unlimited access to target's mobile devices: Remotely and covertly collect information about your target's relationships, location, phone calls, plans and activities – whenever and wherever they are
- Intercept calls: Transparently monitor voice and VoIP calls in real-time
- Bridge intelligence gaps: Collect unique and new types of information (e.g., contacts, files, environmental wiretap, passwords, etc.) to deliver the most accurate and complete intelligence
- Handle encrypted content and devices: Overcome encryption, SSL, proprietary protocols and any hurdle introduced by the complex communications world
- Application monitoring: Monitor a multitude of applications including Skype, WhatsApp, Viber, Facebook and Blackberry Messenger (BBM)
- Pinpoint targets: Track targets and get accurate positioning information using GPS
- Service provider independence: No cooperation with local Mobile Network Operators (MNO) is needed
- Discover virtual identities: Constantly monitor the device without worrying about frequent switching of virtual identities and replacement of SIM cards
- Avoid unnecessary risks: Eliminate the need for physical proximity to the target or device at any phase

Technology Highlights

The Pegasus solution utilizes cutting-edge technology specially developed by veterans of intelligence and law enforcement agencies. It offers a rich set of advanced features and sophisticated intelligence collection capabilities not available in standard interception solutions:

- Penetrates Android, BlackBerry, iOS and Symbian based devices

- Extracts contacts, messages, emails, photos, files, locations, passwords, processes list and more
- Accesses password-protected devices
- Totally transparent to the target
- Leaves no trace on the device
- Minimal battery, memory and data consumption
- Self-destruct mechanism in case of exposure risk
- Retrieves any file from the device for deeper analysis

High Level Architecture

The Pegasus system is designed in layers. Each layer has its own responsibility forming together a comprehensive cyber intelligence collection and analysis solution.

The main layers and building blocks of the systems are:

- Installations: The Installation layer is in charge of issuing new agent installations, upgrading and uninstalling existing agents.
- Data Collection: The Data Collection layer is in charge of collecting the data from the installed device. Pegasus offers comprehensive and complete intelligence by employing four collection methods:
  - – Data Extraction: Extraction of the entire data that exists on the device upon agent installation
  - – Passive Monitoring: Monitor new arrival data to the device
  - – Active Collection: Activate the camera, microphone, GPS and other elements to collect real-time data
  - – Event-based Collection: Define scenarios that automatically triggers specific data collection
- Data Transmission: The Data Transmission layer is in charge of transmitting the collected data back to the command and control servers, using the most efficient and safe way.
- Presentation & Analysis: The Presentation & Analysis component is a User Interface that is in charge of presenting the collected data to the operators and analysts, turning the data into actionable intelligence. This is done using the following modules:
  - – Real-Time Monitoring: Presents real-time collected data from specific or multiple targets. This module is highly important when dealing with sensitive targets or during operational activities, where each piece of information that arrives is crucial for decision making.
  - – Offline Analysis: Advanced queries mechanism that allows the analysts to query and retrieve any piece of information that was collected. The advanced mechanism provides tools to find hidden connections and information.
  - – Geo-based Analysis: Presents the collected data on a map and conduct geo-based queries.
  - – Rules & Alerts: Define rules that trigger alerts based on specific data that arrives or event that occurred.
- Administration: The administration component is in charge of managing the entire system permission, security and health:

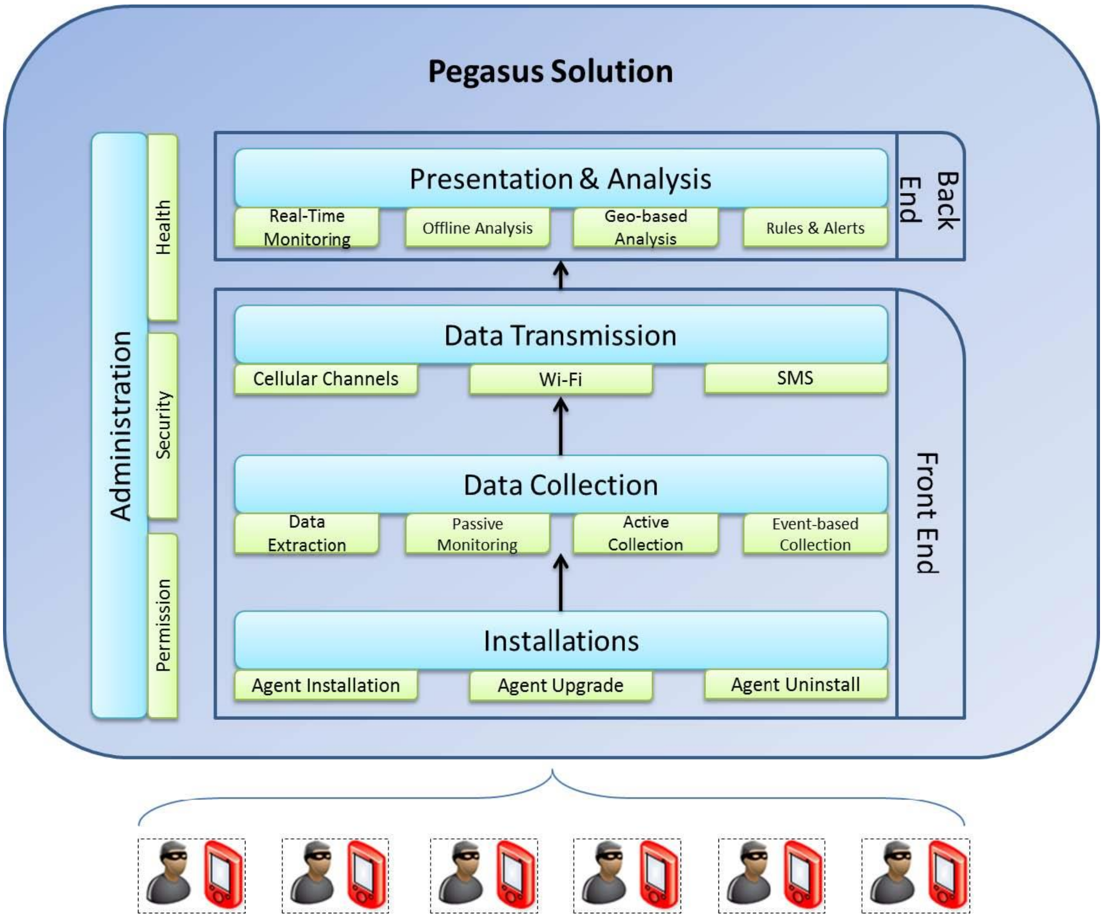
– Permission: The permissions mechanism allows the system administrator to manage the different users of the system. Provide each one of them the right access level only to the data they are allowed to. This allows to define groups in the organization that handle only one or more topics and other groups which handles different topics.

– Security: The security module monitors the system security level, making sure the collected data is inserted to the system database clean and safe for future review.

– Health: The health component of the Pegasus solution monitor the status of all components making sure everything is working smoothly. It monitors the communication between the different parts, the system performance, the storage availability and alerts if something is malfunction.

The system layers and components are shown in Figure 1.

Figure 1: Pegasus High Level Architecture



Agent Installation

In order to start collecting data from your target's smartphone, a software based component ("Agent") must be remotely and covertly installed on their device.

Agent Purpose

The "Agent", a software based component, resides on the end point devices of the monitored targets and its purpose is to collect the data it was configured to. The agent is supported on the most popular operating systems: BlackBerry, Android, iOS (iPhone) and Symbian based devices.

Each agent is independent and is configured to collect different information from the device and to transmit it via specific channels in defined timeframes. The data is sent back to the Pegasus servers in a hidden, compressed and encrypted manner.

The agent continuously collects the information from the device and will transmit it once reliable internet connection becomes available.

Communications encryption, the use of many applications and other communications concealing methods are no longer relevant when an agent is installed on the device.

Agent Installation Vectors

Injecting and installing an agent on the device is the most sensitive and important phase of intelligence operation conducted on the target device. Each installation has to be carefully planned to ensure it is successful. The Pegasus system supports various installation methods. The installation methods variety answers the different operational scenarios which are unique to each customer, resulting in the most comprehensive and flexible solution. Following are the supported installation vectors:

Remote Installation (range free):

- Over-the-Air (OTA): A push message is remotely and covertly sent to the mobile device. This message triggers the device to download and install the agent on the device. During the entire installation process no cooperation or engagement of the target is required (e.g., clicking a link, opening a message) and no indication appears on the device. The installation is totally silent and invisible and cannot be prevented by the target. This is NSO uniqueness, which significantly differentiates the Pegasus solution from any other solution available in the market.

- Enhanced Social Engineering Message (ESEM): In cases where OTA installation method is inapplicable[1], the system operator can choose to send a regular text message (SMS) or an email, luring the target to open it. Single click, either planned or unintentional, on the link will result in hidden agent installation. The installation is entirely concealed and although the target clicked the link they will not be aware that software is being installed on their device.

  The chances that the target will click the link are totally dependent on the level of

[1] e.g., some devices do not support it; some service providers block push messages; target phone number in unknown.

content credibility. The Pegasus solution provides a wide range of tools to compose a tailored and innocent message to lure the target to open the message.

NOTE: Both OTA and ESEM methods require only a phone number or an email address that is used by the target. Nothing else is needed in order to accomplish a successful installation of the Pegasus agent on the device.

Close to the target (range limited):

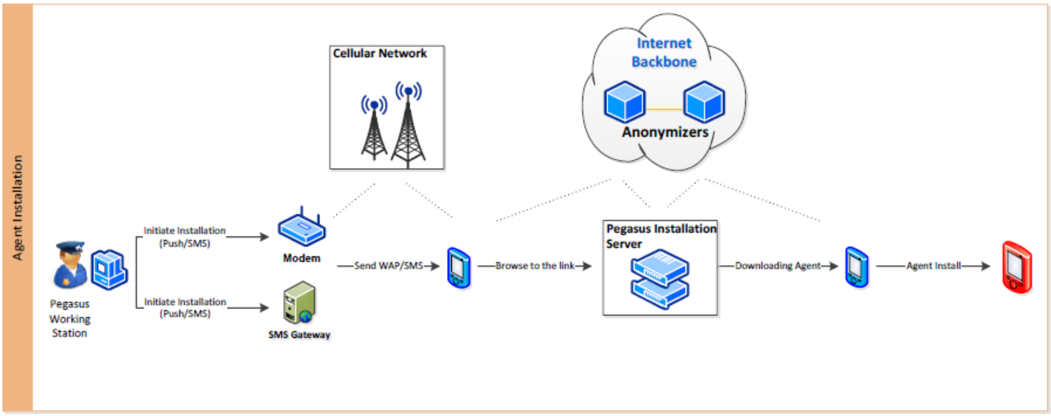
- Tactical Network Element: The Pegasus agent can be silently injected once the number is acquired using tactical network element such as Base Transceiver Station (BTS). The Pegasus solution leverages the capabilities of such tactical tools to perform a remote injection and installation of the agent. Taking a position in the area of the target is, in most cases, sufficient to accomplish the phone number acquisition. Once the number is available, the installation is done remotely.
- Physical: When physical access to the device is an option, the Pegasus agent can be manually injected and installed in less than five minutes. After agent installation, data extraction and future data monitoring is done remotely, providing the same features of any other installation method.

NOTE: Tactical and Physical installations are usually used where no target phone number or email address are available.

Agent Installation Flow

Remote agent installation flow is shown in Figure 2.

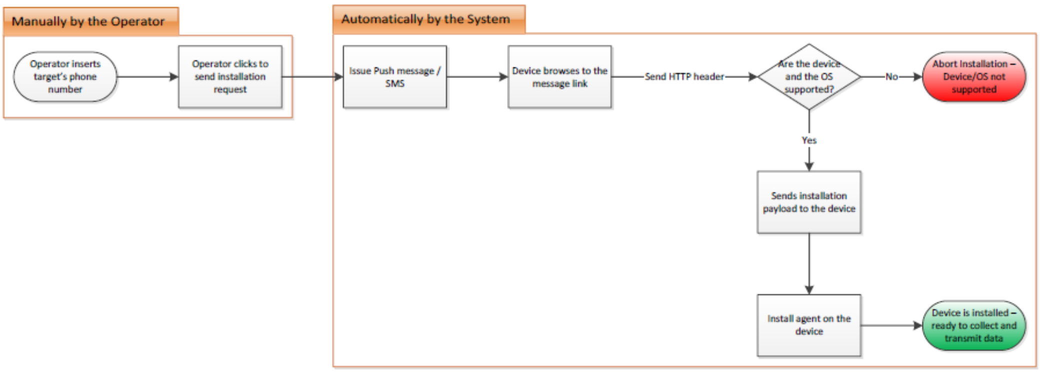
Figure 2: Agent Installation Flow



In order to initiate a new installation, the operator of the Pegasus system should only insert the target phone number. The rest is done automatically by the system, resulting in most cases with an agent installed on the target device.

Agent installation initiation is shown in Figure 3.

Figure 3: Agent Installation Initiation


Manually by the Operator
Operator inserts target's phone number
Operator clicks to send installation request
Automatically by the System
Issue Push message / SMS
Device browses to the message link
Send HTTP header
Are the device and the OS supported?
No
Abort Installation – Device/OS not supported
Yes
Sends installation payload to the device
Install agent on the device
Device is installed – ready to collect and transmit data

Supported Operating Systems & Devices

Operating System (OS)	OS Version	Device	Comments
Android	2.1 – 4.2	▪ Samsung Galaxy series ▪ Sony Ericsson Xperia series ▪ Others (refer to note below)	Support is based on local firmware versions, which must be defined with the customer
iOS	4.x – 6.1.4	▪ iPhone 4 ▪ iPhone 4S ▪ iPhone 5	
BlackBerry	5.0 – 7.1	▪ Curve (8520, 9300, 9350, 9360) ▪ Bold (9000, 9700, 9780, 9790, 9900, 9930) ▪ Torch (9800, 9810, 9850, 9860) ▪ Pearl (9100)	
Symbian	Version S60 OS9 3rd edition FP1, FP2, 5th edition and Symbian^3	Variety of devices	Support is based on local firmware versions, which must be defined with the customer

NOTE: Android-based devices are often added to the supported list. An updated list can be sent upon customer request.

Installation Failure

The installation can sometimes fail due to following reasons:

1. Unsupported device: the target device is not supported by the system (which appears above).

2. Unsupported OS: the operating system of the target device is not supported by the system.

3. Unsupported browser: the default browser of the device was previously replaced by the target. Installation from browsers other than the device default (and also Chrome for Android based devices) is not supported by the system.

In any of the above mentioned cases, if the operator initiates a remote installation to a non-supported device, operating system or browser, the injection will fail and the installation will be aborted. In these cases the process is finished with an open browser on the target device pointing and showing the URL page which was defined by the operator prior the installation.

The device, OS and browser are identified by the system using their HTTP user agent. If by any reason the user agent was manipulated by the target, the system might fail to correctly identify the device and OS and provide the wrong installation payload. In such case, the injection will fail and the installation will be aborted, showing again the above mentioned URL page.

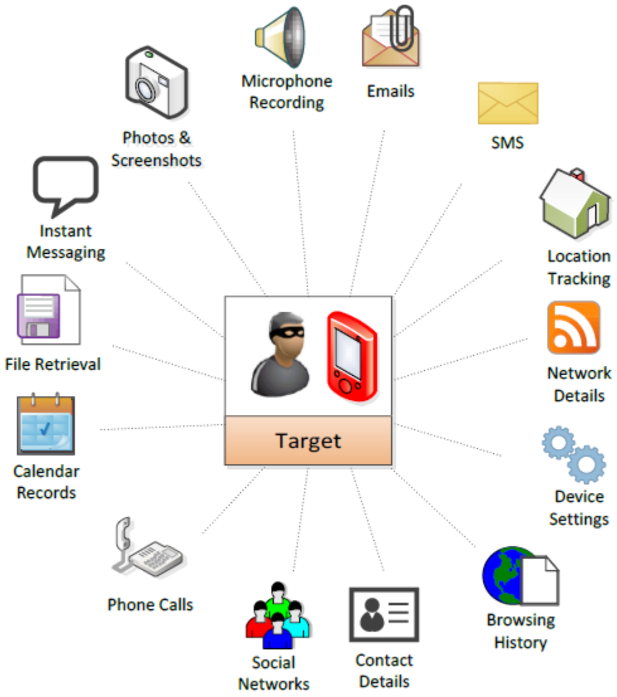
Data Collection

Upon successful agent installation, a wide range of data is monitored and collected from the device:

- Textual: Textual information includes text messages (SMS), Emails, calendar records, call history, instant messaging, contacts list, browsing history and more. Textual information is usually structured and small in size, therefore easier to transmit and analyze.
- Audio: Audio information includes intercepted calls, environmental sounds (microphone recording) and other audio recorded files.
- Visual: Visual information includes camera snapshots, photos retrieval and screen capture.
- Files: Each mobile device contains hundreds of files, some bear invaluable intelligence, such as databases, documents, videos and more.
- Location: On-going monitoring of the device location (Cell-ID and GPS).

The variety of data that is collected by the Pegasus system is shown in Figure 4.

Figure 4: Collected Data



The data collection is divided into three levels:

- Initial data extraction
- Passive monitoring
- Active collection

Initial Data Extraction

Once the agent is successfully injected and installed on the device, the following data that resides and exists on the device can be extracted and sent to the command and control center:

- SMS records
- Contacts details
- Call history (call log)
- Calendar records
- Emails
- Instant Messaging
- Browsing history

As opposed to other intelligence collection solutions which provide only future monitoring of partial communications, Pegasus allows the extraction of all existing data on the device. As a result the organization benefits from accessing historical data about the target, which assists in building a comprehensive and accurate intelligence picture.

NOTE: Initial data extraction is an option and not a must. If the organization is not allowed to access historical data of the target, such option can be disabled and only new arrival data will be monitored by the agent.

Passive Monitoring

From the point the agent was successfully installed it keeps monitoring the device and retrieves any new record that becomes available in real-time (or at specific condition if configured differently). Below is the full list of data that is monitored by the agent:

- SMS records
- Contacts details
- Call history (call log)
- Calendar records
- Emails
- Instant Messaging
- Browsing history
- Location tracking (Cell-ID based)

Active Collection

In addition to passive monitoring, upon successful agent installation a wide set of active collection features becomes available. Active collection refers to active requests sent by the operator to collect specific information from the installed device. These set of features are called active, as they carry their collection upon explicit request of the operator. Active collection allows the operator to perform real-time actions on the target device, retrieving unique information from the device and from the surrounding area of the target, including:

- Location tracking (GPS based)

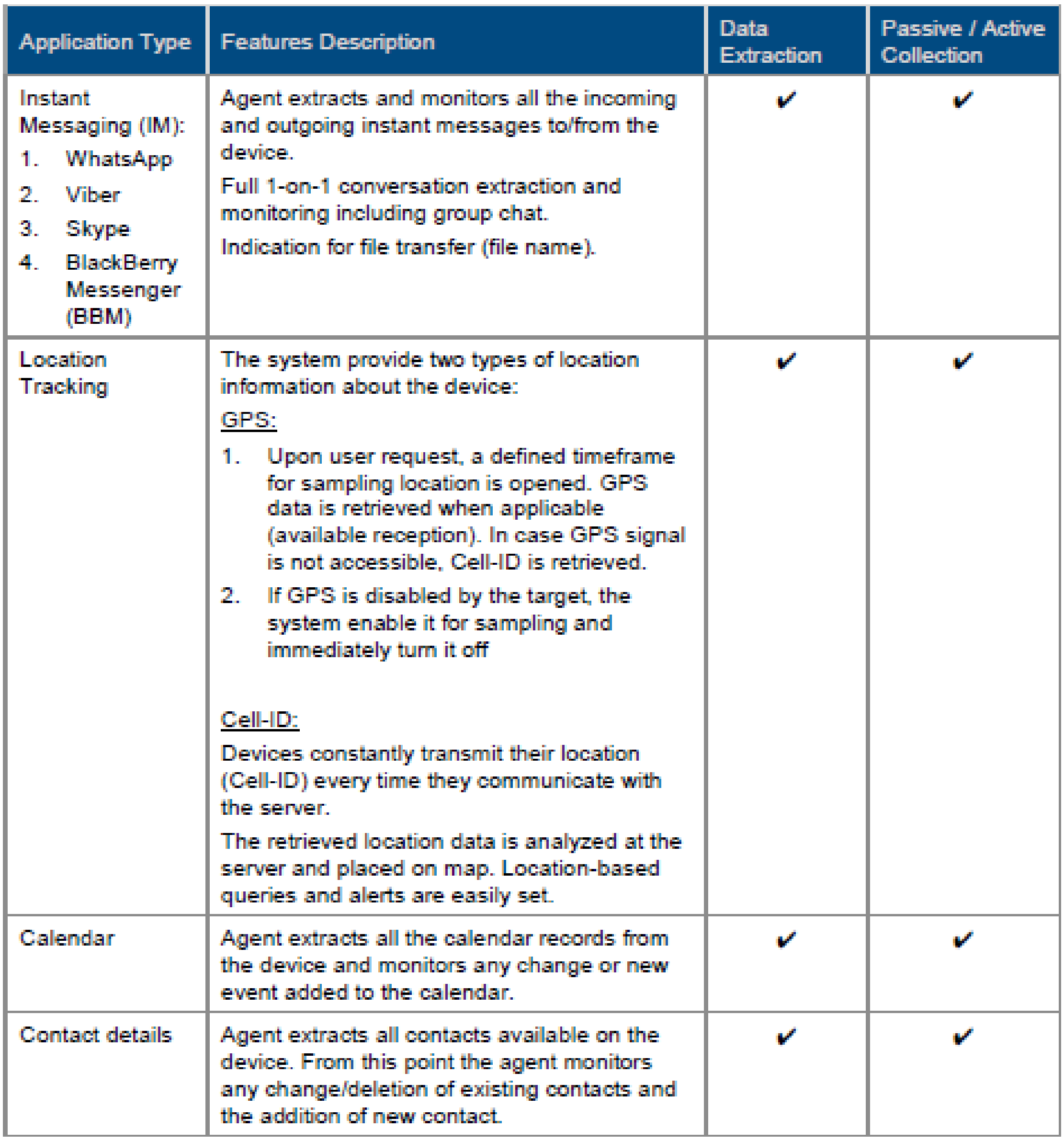
- Voice calls interception
- File retrieval
- Environmental sound recording (microphone recording)
- Photo taking
- Screen capturing

Active collection differentiates Pegasus from any other intelligence collection solution, as the operator controls the information that is collected. Instead of just waiting for information to arrive, hoping this is the information you were looking for, the operator actively retrieves important information from the device, getting the exact information he was looking for.

Description of Collected Data

The different types of data available for extraction, passive monitoring and active collection with their respective features are listed in Table 1.

Table 1: Collection Features Description



Application Type	Features Description	Data Extraction	Passive / Active Collection
Instant Messaging (IM): 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	Agent extracts and monitors all the incoming and outgoing instant messages to/from the device. Full 1-on-1 conversation extraction and monitoring including group chat. Indication for file transfer (file name).	✔	✔
Location Tracking	The system provide two types of location information about the device: GPS: 1. Upon user request, a defined timeframe for sampling location is opened. GPS data is retrieved when applicable (available reception). In case GPS signal is not accessible, Cell-ID is retrieved. 2. If GPS is disabled by the target, the system enable it for sampling and immediately turn it off Cell-ID: Devices constantly transmit their location (Cell-ID) every time they communicate with the server. The retrieved location data is analyzed at the server and placed on map. Location-based queries and alerts are easily set.	✔	✔
Calendar	Agent extracts all the calendar records from the device and monitors any change or new event added to the calendar.	✔	✔
Contact details	Agent extracts all contacts available on the device. From this point the agent monitors any change/deletion of existing contacts and the addition of new contact.	✔	✔

Application Type	Features Description	Data Extraction	Passive / Active Collection
	The agent extracts and monitors all values assigned in each contact field that is available (based on vCard fields), including photo if assigned.		
Environmental sound recording (microphone recording)	The user can request to turn on the device microphone and listen in real-time to the surrounding sounds. The surrounding sounds are recorded and can be analyzed and replayed at a later stage. Turning on the microphone is based on an incoming silent call to the device from the server (PBX). Such call is allowed only after the agent assured that the device is in idle mode (device is not in active use and the screen is turned off). Any action by the target that turns on the screen will result in immediate call hang-up and cease of capturing surrounding sounds. No indication of the recording or the incoming silent call appears on the device at any point. The quality of the recording depends on the device's microphone sensitivity, the surrounding noise and the device model. This sensitivity varies between the different mobile phone models and is set by the phone manufacturer. Usually the content of a conversation held a few meters next to the device can be heard.	N/A[2]	✔
SMS	Agent extracts and monitors all the incoming and outgoing text messages (SMS).	✔	✔
Call Interception (call recording) – Android only	The user can request to record incoming and outgoing calls of the target device. The calls are recorded locally on the device and then sent to the system servers upon completion.	N/A	✔
Email: 1. Main email application in all platforms 2. Gmail application in Android	Agent extracts and monitors all the emails that reside on the device. The main email application (stock) on the device is monitored, thus all accounts which are defined there are monitored (e.g., exchange, Gmail, etc.). For Android-based devices both the main email stock application and the Gmail application are monitored.	✔	✔
File retrieval	Upon user request a full list of files and folders is extracted from the device (internal storage and SD card). When the operator spots a file of interest he can immediately request to retrieve it.	N/A	✔
Photo taking	Upon user request snapshots using the front and rear camera are taken from the device and sent to the servers. The snapshots are taken only after the agent assured that the	N/A	✔

[2] For active collection features, initial data is not extracted before a request is initiated by the user.

Application Type	Features Description	Data Extraction	Passive / Active Collection
	device is in idle mode. During photo taking no indication appears on the device and flash is never used. The quality of the photo can be chosen by the operator to reduce data usage and faster photo transmission. Since flash is not used and the phone might be in motion or inside rooms with low light, the photos are sometimes out of focus.		
Screen capturing	Upon user request a screen capture is taken and sent to the Pegasus servers. The device screenshots can provide insights on the applications used by the target, wallpaper image used and more intimate information about the target.	N/A	✔
Browsing history	Agent extracts and monitors the history of browsed websites from the default browser of the device.	✔	✔
Browsing favorites	Agent extracts and monitors the favorites websites saved in the default browser of the device.	✔	✔
Call history (call log)	Agent extracts the history of all incoming/outgoing calls made to/from the device. The data includes the caller and callee numbers and the duration of the call. Calling attempts which did not result with a conversation will show duration of 0 (zero) seconds.	✔	✔
Device information	Upon agent installation all device, network and connection details are extracted to monitor the general information of the device, including battery level. This provides a summarized view to help understand at-a-glance the device status.	✔	✔

The above mentioned data is the potential data that could be collected by an agent. The agent will collect the data that is applicable and available on the device. If one or more of the above mentioned applications does not exist and/or removed from the device, the agent will operate in the same manner. It will collect the data from the rest of the services and applications which are in use in the device. Also, all the collected data from the removed application will still be saved on the servers or at the agent, if it was not yet transmitted back to the servers.

In addition, the above mentioned data that is collected by the agent covers the most popular applications used worldwide. Since applications popularity differs from country to country, we understands that data extraction and monitoring of other applications will be required as time evolves and new applications are adopted by targets. When such requirement is raised, we can fairly easily extract the important data from virtually any application upon customer demand and release it as a new release that will become available to the customer.

Collection Buffer

The installed agent monitors the data from the device and transmits it to the servers. If transmission is not possible[3] the agent will collect the new available information and transmits it when connection will become available. The collected data is stored in a hidden and encrypted buffer. This buffer is set to reach no more than 5% of the free space available on the device. For example – if the monitored device has 1GB of free space, the buffer can store up to 50MB. In case the buffer has reached its limit, the oldest data is deleted and new data is stored (FIFO). Once the data has been transmitted, the buffer content is totally deleted.

[3] No data channels are available; Device is roaming; Device is shut down.

Data Transmission

By default, the collected data (initial data extraction, passive monitoring and active collection) is sent back to the command and control center in real-time. The data is sent via data channels, where Wi-Fi is the preferred connection to use when it is available. In other cases data is transmitted via cellular data channels (GPRS, 3G and LTE). Extra thought was put into compression methods and focusing on textual content transmission whenever possible. The data footprints are very small and usually take only few hundred bytes. This is to make sure that the collected data is easily transmitted, ensuring minimal impact on the device and on the target cellular data plan.

If data channels are not available, the agent will collect the information from the device and store it in a dedicated buffer, as explained in Data Collection section.

Data transmission is automatically ceased in the following scenarios:

- Low battery: When the device battery level is below the defined threshold (5%) all data transmission processes are immediately ceased until the device is recharged.
- Roaming device: When the device is roaming, cellular data channels become pricy, thus data transmission is done only via Wi-Fi. If Wi-Fi does not exist, transmission will be ceased.

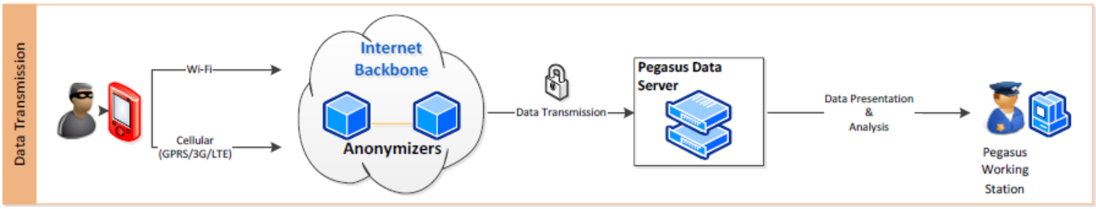
When no data channels are available, and no indication for communication is coming back from the device, the user can request the device will communicate and/or send some crucial data using text messages (SMS).

CAUTION: Communication and/or data transmission via SMS may incur costs by the target and appear in his billing report thus should be used sparingly.

The communication between the agent and the central servers is indirect (through anonymizing network), so trace back to the origin is non-feasible.

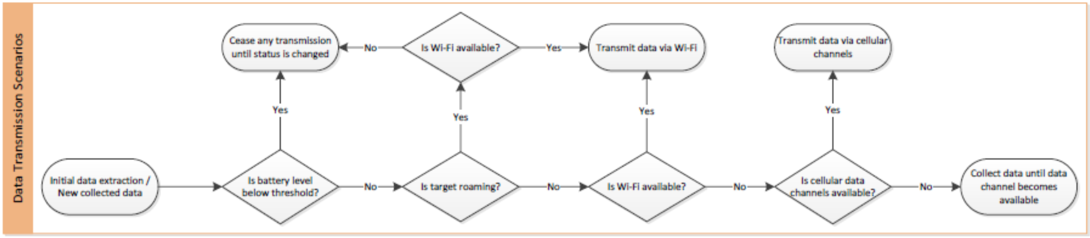
The Pegasus system data transmission process is shown in Figure 5.

Figure 5: Data Transmission Process



The channels and scenarios for transmitting the collected data are shown in Figure 6.

Figure 6: Data Transmission Scenarios


Data Transmission Scenarios
Cease any transmission until status is changed
No
Is Wi-Fi available?
Yes
Transmit data via Wi-Fi
Transmit data via cellular channels
Yes
Yes
Yes
Yes
Initial data extraction / New collected data
Is battery level below threshold?
No
Is target roaming?
No
Is Wi-Fi available?
No
Is cellular data channels available?
No
Collect data until data channel becomes available

Data Transmission Security

All connections between the agents and the servers are encrypted with strong algorithms and are mutually authenticated. While data encryption is probably the most urging issue, extra care was given to ensure minimal data, battery and memory are consumed within the agents requirements. This is meant to make sure that no concerns are raised by the target.

Detecting an operating agent by the target is almost impossible. The Pegasus agent is installed at the kernel level of the device, well concealed and is untraceable by antivirus and antispy software.

The transmitted data is encrypted with symmetric encryption AES 128-bit.

Pegasus Anonymizing Transmission Network

Agent transparency and source security are the guiding principles of the Pegasus solution. To assure that trace back to the operating organization is impossible, the Pegasus Anonymizing Transmission Network (PATN), a network of anonymizers is deployed to serve each customer. The PATN nodes are spread in different locations around the world, allowing agent connections to be redirected through different paths prior to reaching the Pegasus servers. This ensures that the identities of both communicating parties are highly obscured.

Data Presentation & Analysis

Successful data collection from hundreds of targets and devices generates massive amounts of data for visualization, presentation and analysis. The system provides a set of operational tools to help the organization to transform data into actionable intelligence. This is to view, sort, filter, query and analyze the collected data. The tools include:

- Geographical analysis: Track target's real-time and historical location, view several targets on map
- Rules and alerts: Define rules to generate alerts upon important data arrival
- Favorites: Mark important and favorite events for subsequent review and deeper analysis
- Intelligence dashboard: View highlights and statistics of target's activities
- Entity management: Manage targets by groups of interest (e.g., drugs, terror, serious crime, location, etc.)
- Timeline analysis: Review and analyze collected data from a particular time frame
- Advanced search: Conduct search for terms, names, code words and numbers to retrieve specific information

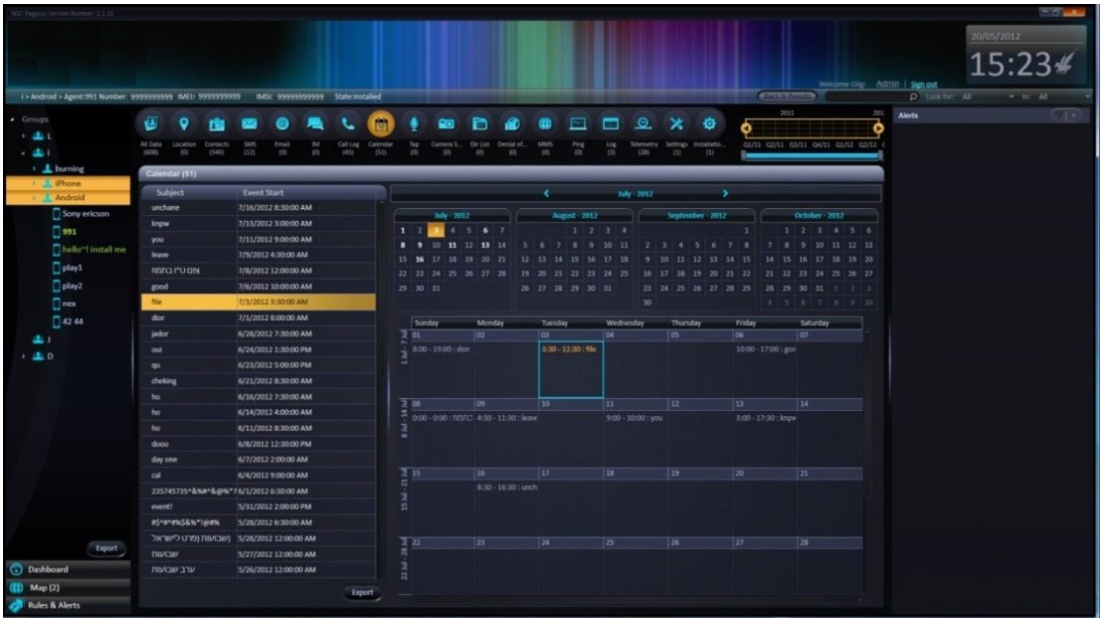
The collected data is organized by groups of interest (e.g., drugs group A, terror group B, etc.) and each group consists of targets. Each target consists of several devices which some have installed agents on them.

The collected data is displayed in an easy-to-use intuitive user interface and when applicable emulates popular display of common applications. The intuitive user interface is designed for a day-to-day work. Operators can easily customize the system to fit their preferred working methods, define rules and alerts for specific topics of interest.

The operator can choose to view the entire collected data from specific target or only specific type of information such as location information, calendar record, emails or instant messages.

Pegasus calendar monitoring screen is shown in Figure 7.

Figure 7: Calendar Monitoring



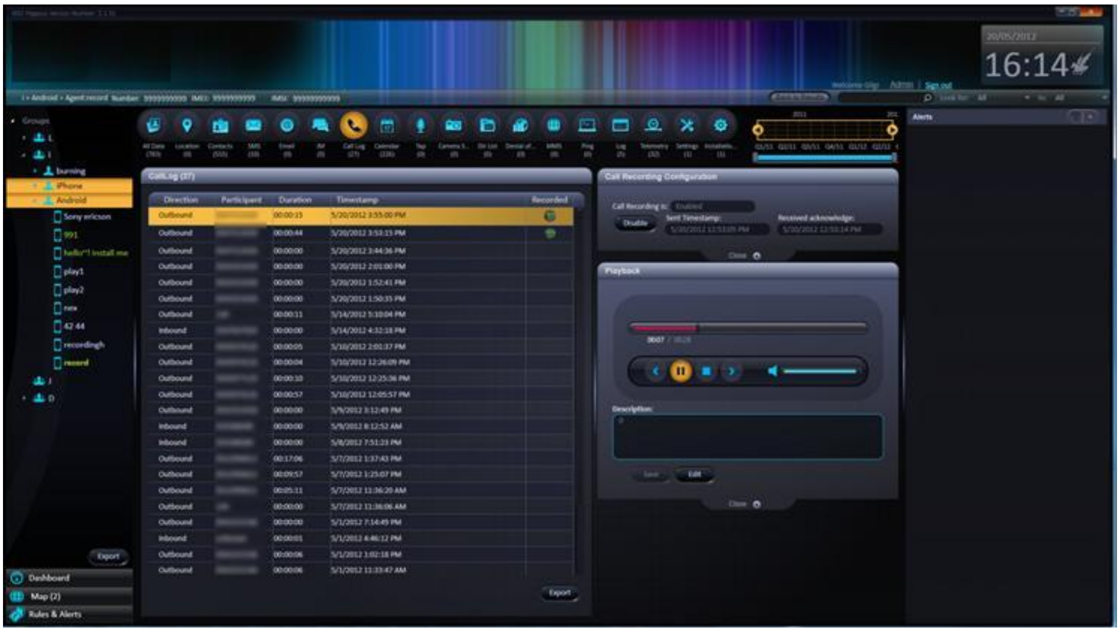
Number: 9999999999 IMEI: 9999999999 IMSI: 99999999999 State:Installed

Calendar (51)

Subject	Event Start
unchane	7/16/2012 8:30:00 AM
knpw	7/13/2012 3:00:00 AM
you	7/11/2012 9:00:00 AM
leave	7/9/2012 4:30:00 AM
צום י"ז בתמוז	7/8/2012 12:00:00 AM
good	7/6/2012 10:00:00 AM
file	7/3/2012 3:30:00 AM
dior	7/1/2012 8:00:00 AM
jador	6/28/2012 7:30:00 AM
oui	6/24/2012 1:30:00 PM
qu	6/23/2012 5:00:00 PM
cheking	6/21/2012 8:30:00 AM
ho	6/16/2012 7:30:00 AM
ho	6/14/2012 4:00:00 AM
ho	6/11/2012 8:30:00 AM
dooo	6/8/2012 12:30:00 PM
day one	6/7/2012 2:00:00 AM
cal	6/4/2012 9:00:00 AM
235745735^&%#^&@%*7	6/1/2012 6:30:00 AM
event!	5/31/2012 2:00:00 PM
#$^#*#%$&%*!@#%	5/28/2012 6:30:00 AM
שבועות (פרט לישראל)	5/28/2012 12:00:00 AM
שבועות	5/27/2012 12:00:00 AM
ערב שבועות	5/26/2012 12:00:00 AM

Pegasus call log and call interception screen is shown in Figure 8.

Figure 8: Call Log & Call Interception

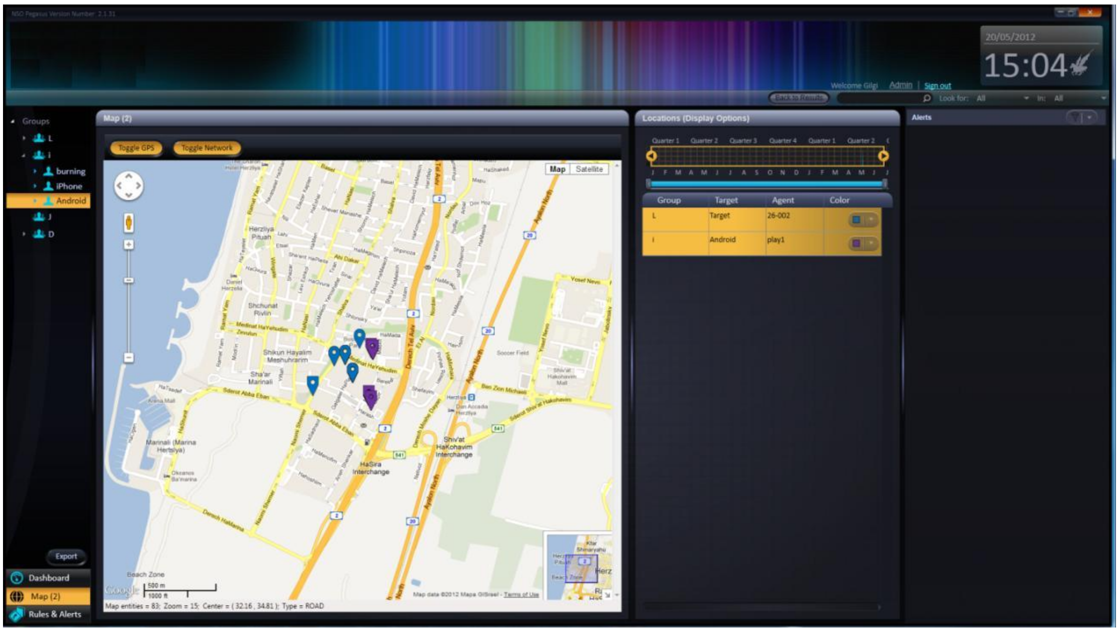


CallLog (27)

Direction	Participant	Duration	Timestamp	Recorded
Outbound	[redacted]	00:00:15	5/20/2012 3:55:00 PM	●
Outbound	[redacted]	00:00:44	5/20/2012 3:53:15 PM	●
Outbound	[redacted]	00:00:00	5/20/2012 3:44:36 PM	
Outbound	[redacted]	00:00:00	5/20/2012 2:01:00 PM	
Outbound	[redacted]	00:00:00	5/20/2012 1:52:41 PM	
Outbound	[redacted]	00:00:00	5/20/2012 1:50:35 PM	
Outbound	[redacted]	00:00:11	5/14/2012 5:10:04 PM	
Inbound	[redacted]	00:00:00	5/14/2012 4:32:18 PM	
Outbound	[redacted]	00:00:05	5/10/2012 2:01:37 PM	
Outbound	[redacted]	00:00:04	5/10/2012 12:26:09 PM	
Outbound	[redacted]	00:00:10	5/10/2012 12:25:36 PM	
Outbound	[redacted]	00:00:57	5/10/2012 12:05:57 PM	
Outbound	[redacted]	00:00:00	5/9/2012 3:12:49 PM	
Inbound	[redacted]	00:00:00	5/9/2012 8:12:52 AM	
Inbound	[redacted]	00:00:00	5/8/2012 7:51:23 PM	
Outbound	[redacted]	00:17:06	5/7/2012 1:37:43 PM	
Outbound	[redacted]	00:09:57	5/7/2012 1:25:07 PM	
Outbound	[redacted]	00:05:11	5/7/2012 11:36:20 AM	
Outbound	[redacted]	00:00:00	5/7/2012 11:36:06 AM	
Outbound	[redacted]	00:00:00	5/1/2012 7:14:49 PM	
Inbound	[redacted]	00:00:01	5/1/2012 4:46:12 PM	
Outbound	[redacted]	00:00:06	5/1/2012 1:02:18 PM	
Outbound	[redacted]	00:00:06	5/1/2012 11:33:47 AM	

Pegasus location tracking screen is shown in Figure 9.

Figure 9: Location Tracking



Group	Target	Agent	Color
L	Target	26-002	
I	Android	play1	

The presentation fields of the collected data are listed in Table 2.

Table 2: Presentation of Collected Data

Service / Application Type	Extracted data	Display method
Instant Messaging (IM): 1. WhatsApp 2. Viber 3. Skype 4. BlackBerry Messenger (BBM)	▪ Chat participants (Names & phones) ▪ Conversation content ▪ Date & Time ▪ Attachments metadata (without the attachment)	▪ Grid ▪ Conversation mode
Location Tracking	▪ Data source (GPS/Cell-ID) ▪ Latitude ▪ Longitude ▪ Date & Time	▪ Grid ▪ Map: - On map display - Full trail - Type of location data (GPS or Cell-ID based)
Calendar	▪ Meeting subject ▪ Event date and start time	▪ Grid ▪ Monthly calendar view (emulates popular calendar clients)
Contact details	▪ Entire values stored in the contact entry including photo if available	▪ Grid ▪ Contact card with the entire details
Environmental sound recording (microphone recording)	▪ Recorded audio ▪ Recording Date & Time ▪ Duration	▪ Grid ▪ Playback interface
SMS	▪ Direction (incoming, outgoing) ▪ Contact name ▪ Phone number ▪ Message content ▪ Date & Time	▪ Grid
Call Interception	▪ Direction ▪ Contact name ▪ Phone number ▪ Duration ▪ Date & Time	▪ Grid ▪ Playback interface
Email: 1. Main email application in all platforms 2. Gmail application in Android	▪ From ▪ To ▪ CC ▪ BCC ▪ Subject ▪ Folder ▪ Account ▪ Message content ▪ Date & Time	▪ Grid ▪ HTML (emulates popular email clients)
File retrieval	▪ List of folders (tree) ▪ List of files (grid): ▪ Filename	▪ Grid ▪ Tree view

Service / Application Type	Extracted data	Display method
	Modified date File size	
Photo taking	Date & Time Photo	Grid Photo viewer
Screen capturing	Date & Time Screen capture image	Grid Photo viewer
Browsing history	Website name (as saved by the target, usually the default website name) Website URL address	List
Browsing favorites	Website name (as saved by the target, usually the default website name) Website URL address	List
Call history (call log)	Direction Contact name Phone number Duration Date & Time	Grid
Device information	Battery level Connection type (e.g., 3G, WiFi) MSISDN IMEI IMSI Device Manufacturer Device model Operating System version Installation date Last communication time Device current country Device home country Serving network Home serving network	Dashboard

Rules & Alerts

The Rules & Alerts module in the system alerts when important event takes place. Rules must be defined in advance and they help the operators to review and take actions in real-time, for example:

- Geo-fencing:
  - Access hot zone - Alert when target reached an important location
  - Leave hot zone - Alert when target left a certain location

  Geo-fence alerts are based on a perimeter around a certain location, where the operator defines the size of the perimeter.
- Meeting detection: Alert when two targets meet (share the same location)

- Connection detection:
  - Alert when a message is sent from/to a specific number
  - Alert when a phone call is performed from/to a specific number
- Content detection: Alert when a defined word/term/code word is used in a message

Data Export

The system is designed as an end-to-end system, providing its users with collection and analysis tools. However, we understands that there are advanced analysis capabilities and data fusion requirements from other sources, therefore the system allows the exporting of the collected information and seamless integration with 3rd party backend or analysis systems available.

Agent Maintenance

Once agent is installed on a certain device, it has to be maintained in order to support new features and change its settings and configurations or to be uninstalled when it is no longer providing valuable intelligence to the organization.

Agent Upgrade

When agents' updates are released they become available to install. These new agents are now ready for installation on new targets' devices or as upgrades for existing agents installed on target's devices. These updates provide new functionalities, bug fixing, support for new services or improve the agents overall behavior. Such updates are crucial to keep the agent functional and operational in the endless progress of the communication world and especially the smartphone arena.

There are two types of agent upgrades:

- Optional upgrade: agent upgrade is not mandatory by the system. The user decides when, if at all, to upgrade the agent.
- Mandatory upgrade: agent upgrade is mandatory by the system. The supervisor must upgrade the agent otherwise no new information will be monitored from the device.

Upgrade sometimes requires an installation of a new agent and sometimes just a small update of the existing agent. In both cases the user is the only one to decide when to conduct the upgrade, and therefore should plan this accordingly.

Once the command for upgrade was sent by the user, the process should take only few minutes. The process might take longer if the device is turned off or has bad data connection. In either case, the upgrade will be accomplished once a decent data connection becomes available.

Agent Settings

Agent settings are set for the first time during its installation. From this point, these settings serve the agent, but can always be changed if required. The settings include the IP address for transmitting the collected data, the way commands are sent to the agent, the time until the agent is automatically uninstall itself (see self-destruct mechanism for more details) and more.

Agent Uninstall

When the intelligence operation is done or in case where the target is no longer with interest to the organization, the software based component ("Agent") on the target's device can be removed and uninstalled. Uninstall is quick, requires a single user request and has no to minimal effect on the target device. The user issues a request for agent uninstall which is sent to the device.

Once agent is uninstalled from a certain device it leaves no traces whatsoever or indications it was ever existed there[4]. As long as the agent is operational on the device and a connection exists between him and the servers it can be easily and remotely uninstalled.

.

Uninstall can always be done remotely no matter what was the method used for installation. Physical uninstall is also an option, if needed.

Uninstalling an agent does not mean losing the entire collected data – the entire data that was collected during the time that the agent was installed on the device will be kept in the servers for future analysis.

Self-Destruct Mechanism

The Pegasus system contains self-destruct mechanism for the installed agents. In general, we understand that it is more important that the source will not be exposed and the target will suspect nothing than keeping the agent alive and working. The mechanism is activated in the following scenarios:

- Risk of exposure: In cases where a great probability of exposing the agent exists, a self-destruct mechanism is automatically being activated and the agent is uninstalled. Agent can be once again installed at a later time.
- Agent is not responding: In cases where the agent is not responding and did not communicate with the servers for a long time[5], the agent will automatically uninstall itself to prevent being exposed or misused.

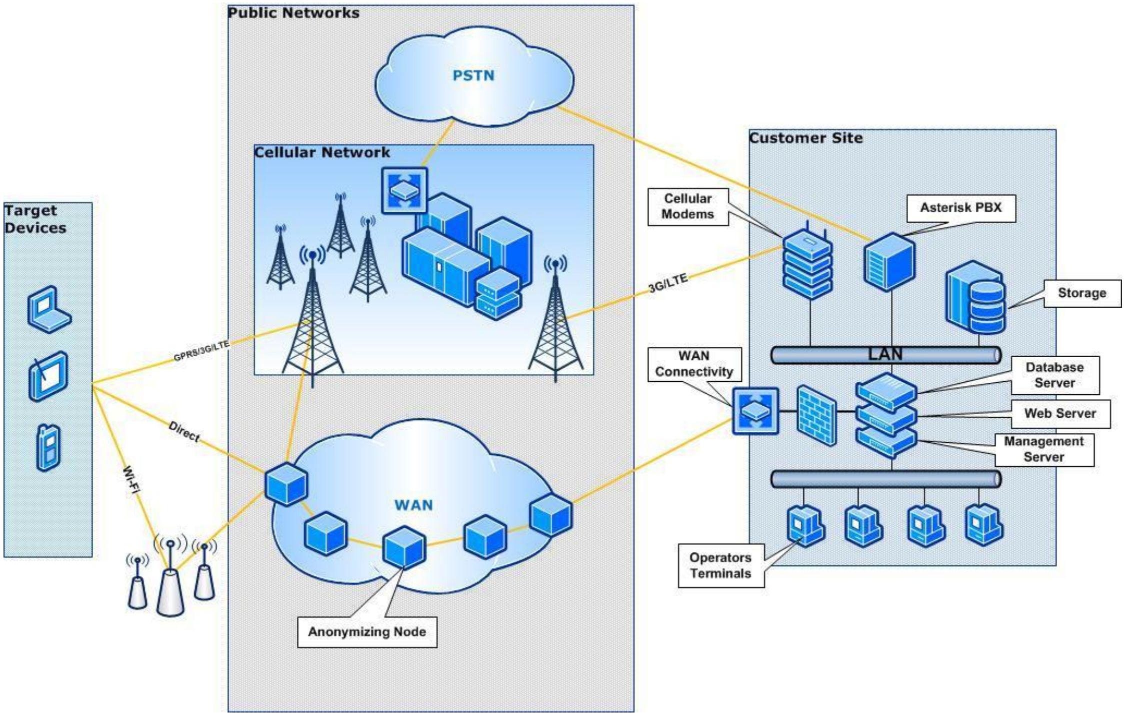
[4] In some cases, uninstall can result in device reboot. If reboot takes place, it happens once agent removal is done. The device comes up clean with no agent installed.

[5] The default time is 60 days, but can be reconfigured for any period of time required

Solution Architecture

The Pegasus system's major architectural components are shown in Figure 10.

Figure 10: Solution Architecture



Customer Site

NSO is responsible to deploy and configure the Pegasus hardware and software at the customer premises, making sure the system is working and functioning properly. Below are the main components installed at the customer site:

WEB Servers

Residing at the customer's premises, the servers are responsible for the following:

- Agent installation and monitoring
- Agent maintenance: Remotely control, configure and upgrade installed agents
- Data transmission: Receive the collected data transmitted from the installed agents
- Serve the operators' terminals

Communications Module

The communications module allows interconnectivity and internet connection to the servers.

Cellular Communication Module

The cellular communication module enables remote installation of the Pegasus agent to the target device using cellular modems and/or SMS gateways.

Permission Module

The Pegasus permission management module defines and controls the features and available content allowed for each user based on their role, rank and hierarchy.

Data Storage

The collected data that was extracted and monitored by the agents is stored on an external storage device. The data is well backed-up and with full resiliency and redundancy to prevent failures and downtime.

Servers Security

All the servers reside inside the customer's trusted network, behind any security measures it may deploy as well as security measures that we supply specifically for the system.

Hardware

The system standard hardware is deployed on several servers connected together on couple of racks. The equipment takes care of advanced load balancing, content compression, connection management, encryption, advanced routing, and highly configurable server health monitoring.

Operator Consoles

The operator's end-point terminals (PC) are the main tool which the operators activate the Pegasus system, initiate installations and commands, and view the collected data.

Pegasus Application

The Pegasus application is the user interface that is installed on the operator terminal. It provides the operators with range of tools to view, sort, filter, manage and alert to analyze the large amount of data collected from the targets' agents.

Public Networks

Apart from local hardware and software installation at the customer premises, the Pegasus system does not require any physical interface with the local mobile network operators. However, since agent installations and data are transferred over the public networks, we makes sure it is transferred in the most efficient and secured way, all the way back to the customer servers:

Anonymizing Network

Pegasus Anonymizing Transmission Network (PATN) is built from anonymizing connectivity nodes which are spread in different locations around the world, allowing agent connections to be directed through different paths prior to reaching the Pegasus servers. The anonymized nodes serve only one customer and can be set up by the customer if required.

See more information in Pegasus Anonymizing Transmission Network section.

Target Devices

The above mentioned architecture allows the operators to issue new installations, extract, monitor and actively collect data from targets' devices. See more details in Supported Operating Systems & Devices.

NOTE: The Pegasus is an intelligence mission-critical system, therefore it is fully redundant to avoid malfunctions and failures. The system handles large amounts of data and traffic 24 hours a day and is scalable to support customer growth and future requirements.

Solution Hardware

The hardware specifications for operating the Pegasus system depends on the number of concurrent installed agents, the number of working stations, the amount of data stored and for how long should it be stored.

All the necessary hardware is supplied with the system upon deployment and may require local customization that has to be handled by the customer based on we directions. If required, hardware can be purchased by the customer based on the specifications provided by we.

Operators Terminals

The operator terminals are standard desktop PCs, with the following specifications:

- Processor: Core i5
- Memory: 3GB RAM
- Hard Drive: 320GB
- Operating System: Windows 7

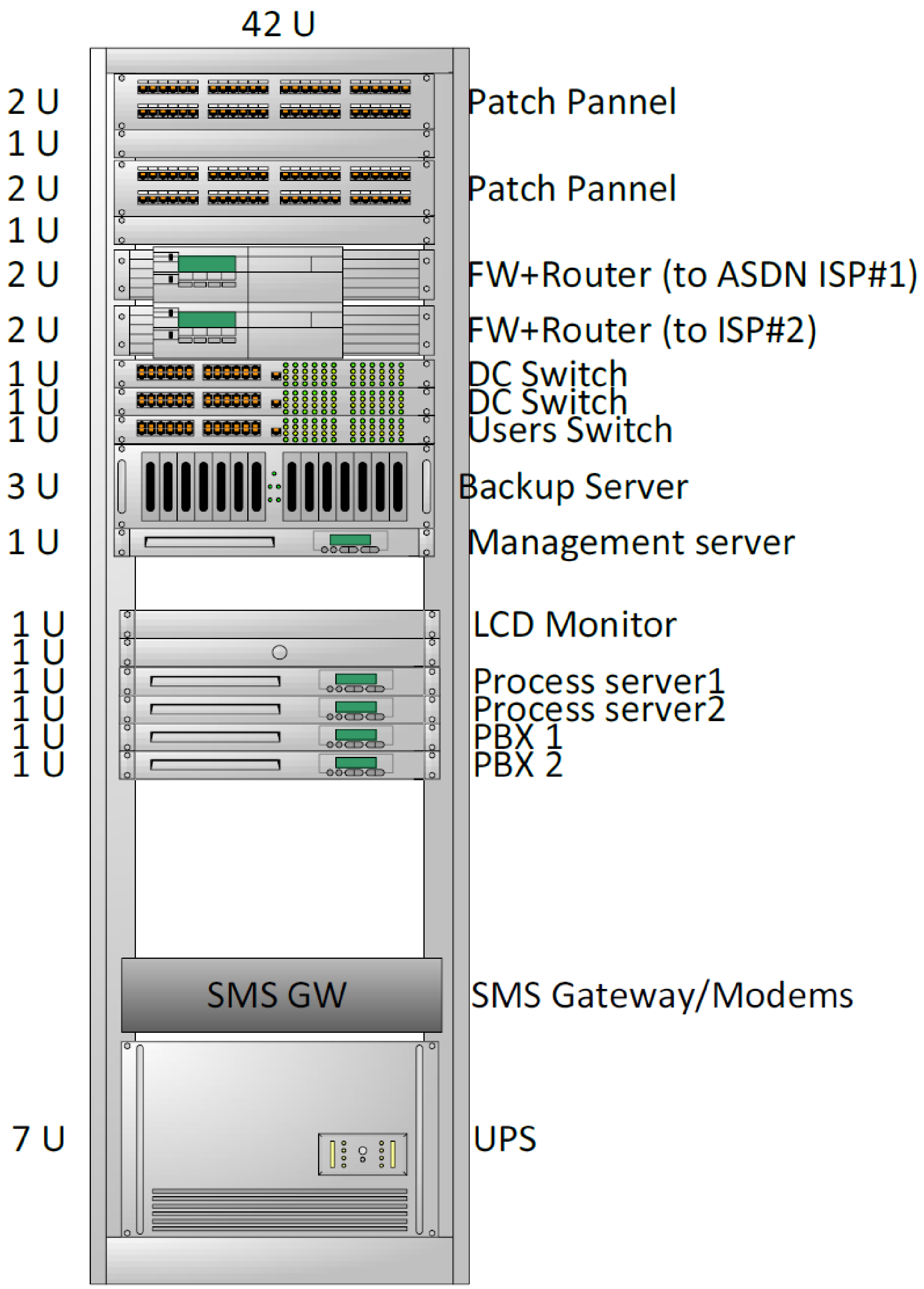
System Hardware

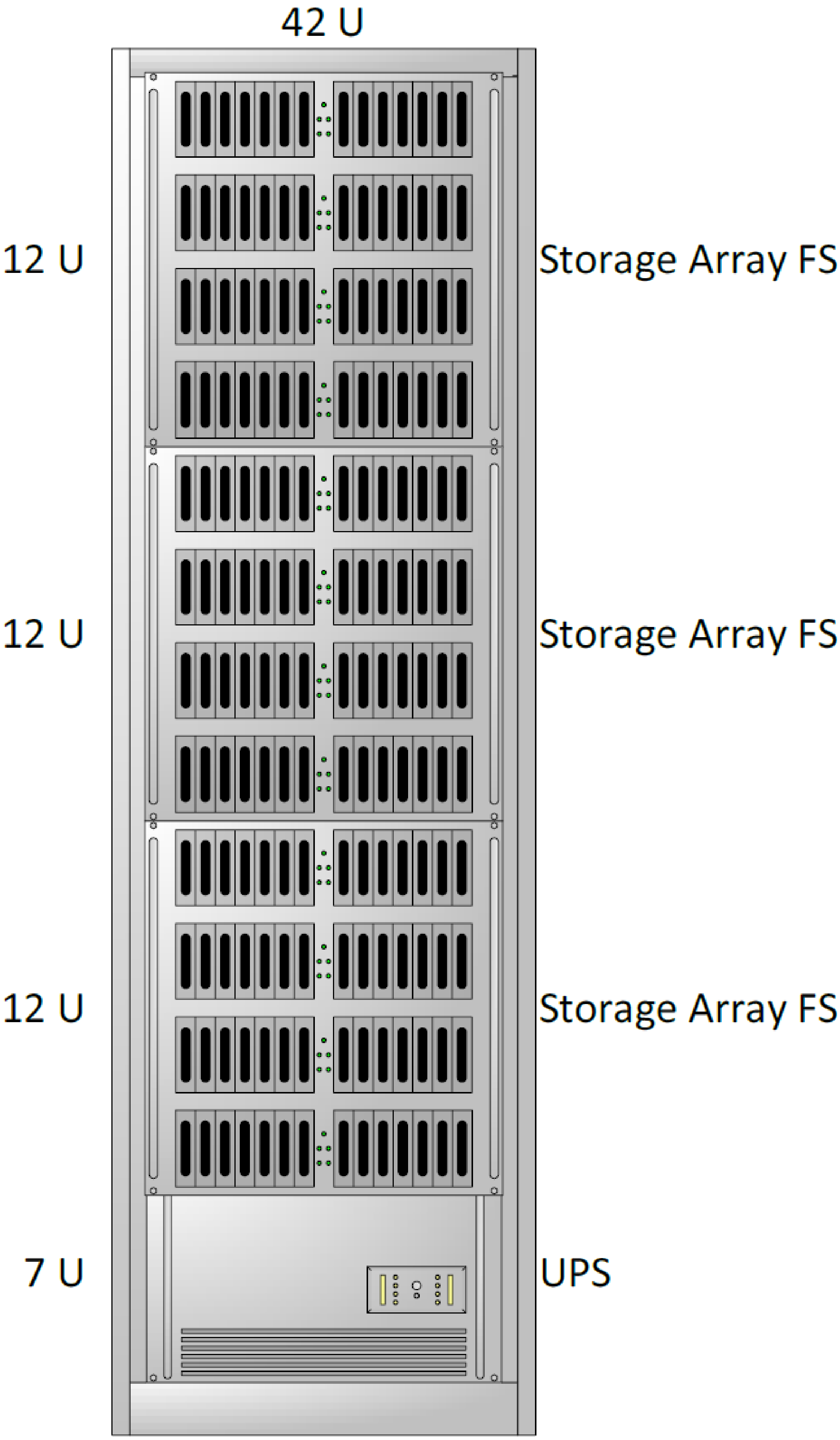
To fully support the system infrastructure, the following hardware is required:

- Two units of 42U cabinet
- Networking hardware
- 10TB of storage
- 5 standard servers
- UPS
- Cellular modems and SIM cards

The system hardware scheme is shown in Figure 11.

Figure 11: Pegasus Hardware




42 U
12 U
Storage Array FS
12 U
Storage Array FS
12 U
Storage Array FS
7 U
UPS

System Setup and Training

We are responsible for the system setup and training before its hand-over to the customer.

System Prerequisites

Successful installation of the Pegasus system requires the following preparations of the servers' room:

- Sufficient room to contain two 42U racks cabinet, 5x5x2.5m (LxWxH)
- Air conditioned (18°C) room
- Access restriction
- Routing from end-point terminals to servers room
- Reliable cellular network reception (at least -95 dBm)
- 2 x Electrical outlets (20A) per rack
- 2 x Symmetric ATM lines from different ISP's. Each line with a bandwidth of 10MB containing 8 external static IP addresses:
    - ISP #1: Fiber optic-based network
    - ISP #2: Ethernet category-7 cable-based network

  The mission-critical system requires two parallel networks to ensure system resilience and downtime is kept to an absolute minimum.
- 2 x E1 PRI connections, each contains 10 extensions (two different service providers is recommended)
- 2 x anonymous SIM cards for each local Mobile Network Operator
- 3rd party services registration as required

System Setup

- The solution will be deployed at the customer site by we personnel
- Deployment duration usually requires 10-15 working weeks
- Operating environment prerequisites must be met
- System setup includes hardware and software installation, and in addition integration to local environment and systems
- Support and adaptations to the different local device firmware versions

Training

Upon system installation, we personnel will conduct full training sessions. Training can take place onsite or in any other location required by the customer, including we headquarters. Training session includes the following:

- Basic system usage
- System architecture
- Advanced system usage and roles

- Real-world simulation exercises

The recommended number of attendees is with respect to the number of installed operator consoles.

High Level Deployment Plan

The process of adapting, installing and testing the system in a new customer site in listed in Table 3.

Table 3: Pegasus Deployment Plan

<table>
<tr><th>Week
Phase</th><th>1</th><th>2</th><th>3</th><th>4</th><th>5</th><th>6</th><th>7</th><th>8</th><th>9</th><th>10</th><th>11</th><th>12</th><th>13</th><th>14</th><th>15</th></tr>
<tr><td rowspan="3">Phase 1 - Preparations</td><td>ATP req.</td><td colspan="6">Equipment acquisition</td><td colspan="8"></td></tr>
<tr><td></td><td colspan="6">System Integration</td><td colspan="8"></td></tr>
<tr><td colspan="2"></td><td colspan="4">Local Networks Adjustments</td><td colspan="9"></td></tr>
<tr><td rowspan="3">Phase 2 - Implementation</td><td colspan="5"></td><td colspan="5">System Testing</td><td colspan="5"></td></tr>
<tr><td colspan="7"></td><td colspan="2">HW Installation</td><td colspan="6"></td></tr>
<tr><td colspan="8"></td><td colspan="7">Device Porting Process</td></tr>
<tr><td rowspan="2">Phase 3 – Training &amp; Completion</td><td colspan="11"></td><td colspan="2">System Training</td><td colspan="2"></td></tr>
<tr><td colspan="13"></td><td colspan="2">Customer ATP</td></tr>
</table>

Phase 1 – Preparations:

- Requirements for an Acceptance Test Procedure (ATP) are defined together with the customer
- Hardware and software acquisition and customization to answer customer requirements and needs
- When required, the Pegasus system is integrated with local infrastructures and systems
- System adaptations to the local mobile networks

Phase 2 – Implementation:

- System testing
- Hardware installation
- System adaptations to local device firmware versions

Phase 3 – Training and Completion:

- Detailed system training, real-life scenarios practicing and simulation
- Customer ATP as defined during phase 1

System Acceptance Test (SAT)

We have gained substantial experience in installing and implementing the Pegasus system. The following acceptance test plan verifies that the system works as required and validates that the correct functionality has been delivered. It describes the scope of the work to be performed and the approach taken to execute the proper tests to validate that the system functions as mutually agreed with the customer.

The tests are divided into 3 stages:

- Functionality tests
- Network and providers tests
- Customer tailor specific tests

An official system hand-over from we to the customer is done once the system has been deployed, tested and demonstrated.

Maintenance, Support and Upgrades

We provides, as default, one year of maintenance, support and upgrades services. These services include:

Maintenance and Support

We provides maintenance services and three-tier level support that includes:

- Tier-1: Standard system operations problems
  - ○ Email and phone support
- Tier-2: Proactive resolving of technical problems
  - ○ Dedicated engineers will inspect, examine and resolve common technical issues, putting their best efforts
  - ○ Remote assistance using remote desktop software and a Virtual Private Network (VPN) where requested
- Tier-3: Bug fixing and system updates of substantial system malfunctions
- Phone support: In addition to the above mentioned, we provide phone and email support to any question and problem that is raised.

In addition, the customer will be able to add the following support:

- Planned or emergency onsite assistance
- Health monitoring system

Upgrades

We have releases major upgrades to the Pegasus system few times a year. Such upgrades usually include:

- New features
- New devices/operating system support
- Tailored features based on customer requirements
- Bugs fix

JS 44 (Rev. 09/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

HANAN ELATR KHASHOGGI,

(b) County of Residence of First Listed Plaintiff Fairfax County, VA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Steven T. Webster, Webster Book LLP,
300 N Washington St, Ste 404, Alexandria, VA 22314,
(888) 987-9991, swebster@websterbook.com

DEFENDANTS

NSO GROUP TECHNOLOGIES LIMITED and
Q CYBER TECHNOLOGIES LIMITED

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

□ 1 U.S. Government Plaintiff	☒ 3 Federal Question *(U.S. Government Not a Party)*
□ 2 U.S. Government Defendant	□ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	□ 1	□ 1	Incorporated *or* Principal Place of Business In This State	□ 4	□ 4
Citizen of Another State	□ 2	□ 2	Incorporated *and* Principal Place of Business In Another State	□ 5	□ 5
Citizen or Subject of a Foreign Country	□ 3	□ 3	Foreign Nation	□ 6	□ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- □ 110 Insurance
- □ 120 Marine
- □ 130 Miller Act
- □ 140 Negotiable Instrument
- □ 150 Recovery of Overpayment & Enforcement of Judgment
- □ 151 Medicare Act
- □ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- □ 153 Recovery of Overpayment of Veteran's Benefits
- □ 160 Stockholders' Suits
- □ 190 Other Contract
- □ 195 Contract Product Liability
- □ 196 Franchise

REAL PROPERTY
- □ 210 Land Condemnation
- □ 220 Foreclosure
- □ 230 Rent Lease & Ejectment
- □ 240 Torts to Land
- □ 245 Tort Product Liability
- □ 290 All Other Real Property

TORTS

PERSONAL INJURY
- □ 310 Airplane
- □ 315 Airplane Product Liability
- □ 320 Assault, Libel & Slander
- □ 330 Federal Employers' Liability
- □ 340 Marine
- □ 345 Marine Product Liability
- □ 350 Motor Vehicle
- □ 355 Motor Vehicle Product Liability
- ☒ 360 Other Personal Injury
- □ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- □ 365 Personal Injury - Product Liability
- □ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- □ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- □ 370 Other Fraud
- □ 371 Truth in Lending
- □ 380 Other Personal Property Damage
- □ 385 Property Damage Product Liability

CIVIL RIGHTS
- □ 440 Other Civil Rights
- □ 441 Voting
- □ 442 Employment
- □ 443 Housing/ Accommodations
- □ 445 Amer. w/Disabilities - Employment
- □ 446 Amer. w/Disabilities - Other
- □ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- □ 463 Alien Detainee
- □ 510 Motions to Vacate Sentence
- □ 530 General
- □ 535 Death Penalty

Other:
- □ 540 Mandamus & Other
- □ 550 Civil Rights
- □ 555 Prison Condition
- □ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- □ 625 Drug Related Seizure of Property 21 USC 881
- □ 690 Other

LABOR
- □ 710 Fair Labor Standards Act
- □ 720 Labor/Management Relations
- □ 740 Railway Labor Act
- □ 751 Family and Medical Leave Act
- □ 790 Other Labor Litigation
- □ 791 Employee Retirement Income Security Act

IMMIGRATION
- □ 462 Naturalization Application
- □ 465 Other Immigration Actions

BANKRUPTCY
- □ 422 Appeal 28 USC 158
- □ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- □ 820 Copyrights
- □ 830 Patent
- □ 835 Patent - Abbreviated New Drug Application
- □ 840 Trademark

SOCIAL SECURITY
- □ 861 HIA (1395ff)
- □ 862 Black Lung (923)
- □ 863 DIWC/DIWW (405(g))
- □ 864 SSID Title XVI
- □ 865 RSI (405(g))

FEDERAL TAX SUITS
- □ 870 Taxes (U.S. Plaintiff or Defendant)
- □ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- □ 375 False Claims Act
- □ 376 Qui Tam (31 USC 3729(a))
- □ 400 State Reapportionment
- □ 410 Antitrust
- □ 430 Banks and Banking
- □ 450 Commerce
- □ 460 Deportation
- □ 470 Racketeer Influenced and Corrupt Organizations
- □ 480 Consumer Credit (15 USC 1681 or 1692)
- □ 485 Telephone Consumer Protection Act
- □ 490 Cable/Sat TV
- □ 850 Securities/Commodities/ Exchange
- □ 890 Other Statutory Actions
- □ 891 Agricultural Acts
- □ 893 Environmental Matters
- □ 895 Freedom of Information Act
- □ 896 Arbitration
- □ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- □ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding □ 2 Removed from State Court □ 3 Remanded from Appellate Court □ 4 Reinstated or Reopened □ 5 Transferred from Another District *(specify)* □ 6 Multidistrict Litigation - Transfer □ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
18 U.S.C. § 1030 et seq.

Brief description of cause:
Computer Fraud and Abuse Act and associated state law claims.

VII. REQUESTED IN COMPLAINT:

□ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes □ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE DOCKET NUMBER

DATE
06/15/2023

SIGNATURE OF ATTORNEY OF RECORD
/s/ Steven T. Webster

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE