COOLEY LLP
TRAVIS LEBLANC (251097) (tleblanc@cooley.com)
JOSEPH D. MORNIN (307766) (jmornin@cooley.com)
101 California Street, 5th floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

DANIEL J. GROOMS (D.C. Bar No. 219124) (*pro hac vice* forthcoming)
(dgrooms@cooley.com)
1299 Pennsylvania Avenue, NW, Suite 700
Washington, DC 20004-2400
Telephone: (202) 842-7800
Facsimile: (202) 842-7899

Attorneys for Plaintiffs
WHATSAPP INC. and FACEBOOK, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC., a Delaware corporation, and FACEBOOK, INC., a Delaware corporation, Plaintiffs, v. NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED, Defendants.	Case No. **COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs WhatsApp Inc. and Facebook, Inc. (collectively, "Plaintiffs") allege the following against Defendants NSO Group Technologies Ltd. ("NSO Group") and Q Cyber Technologies Ltd. ("Q Cyber") (collectively, "Defendants"):

INTRODUCTION

1. Between in and around April 2019 and May 2019, Defendants used WhatsApp servers, located in the United States and elsewhere, to send malware to approximately 1,400 mobile phones and devices ("Target Devices"). Defendants' malware was designed to infect the Target Devices for the purpose of conducting surveillance of specific WhatsApp users ("Target Users"). Unable to break WhatsApp's end-to-end encryption, Defendants developed their malware in order to access messages and other communications after they were decrypted on Target Devices. Defendants' actions were not authorized by Plaintiffs and were in violation of WhatsApp's Terms of Service. In May 2019, Plaintiffs detected and stopped Defendants' unauthorized access and abuse of the WhatsApp Service and computers.

2. Plaintiffs bring this action for injunctive relief and damages pursuant to the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502, and for breach of contract and trespass to chattels.

PARTIES

3. Plaintiff WhatsApp Inc. ("WhatsApp") is a Delaware corporation with its principal place of business in Menlo Park, California.

4. Plaintiff Facebook, Inc. ("Facebook") is a Delaware corporation with its principal place of business in Menlo Park, California. Facebook acts as WhatsApp's service provider for security-related issues.

5. Defendant NSO Group was incorporated in Israel on January 25, 2010, as a limited liability company. Ex. 1. NSO Group had a marketing and sales arm in the United States called WestBridge Technologies, Inc. Ex. 2 and 3. Between 2014 and February 2019, NSO Group obtained financing from a San Francisco–based private equity firm, which ultimately purchased a controlling stake in NSO Group. Ex. 4. In and around February 2019, NSO Group was reacquired by its founders

and management. *Id.* NSO Group's annual report filed on February 28, 2019, listed Defendant Q Cyber as the only active director of NSO Group and its majority shareholder. Ex. 5.

6. Defendant Q Cyber was incorporated in Israel on December 2, 2013, under the name L.E.G.D. Company Ltd. Ex. 6 and 7. On May 29, 2016, L.E.G.D. Company Ltd. changed its name to Q Cyber. Ex. 7. Until at least June 2019, NSO Group's website stated that NSO Group was "a Q Cyber Technologies company." Ex. 8. Q Cyber's annual report filed on June 17, 2019, listed OSY Technologies S.A.R.L. as the only Q Cyber shareholder and active Director. Ex. 9

7. At all times material to this action, each Defendant was the agent, partner, alter ego, subsidiary, and/or coconspirator of and with the other Defendant, and the acts of each Defendant were in the scope of that relationship. In doing the acts and failing to act as alleged in this Complaint, each Defendant acted with the knowledge, permission, and consent of each other; and, each Defendant aided and abetted each other.

JURISDICTION AND VENUE

8. The Court has federal question jurisdiction over the federal causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1331.

9. The Court has supplemental jurisdiction over the state law causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1367 because these claims arise out of the same nucleus of operative fact as Plaintiffs' federal claims.

10. In addition, the Court has jurisdiction over all the causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1332 because complete diversity between the Plaintiffs and each of the named Defendants exists, and because the amount in controversy exceeds $75,000.

11. The Court has personal jurisdiction over Defendants because they obtained financing from California and directed and targeted their actions at California and its residents, WhatsApp and Facebook. The claims in this Complaint arise from Defendants' actions, including their unlawful access and use of WhatsApp computers, several of which are located in California.

12. The Court also has personal jurisdiction over Defendants because Defendants agreed to WhatsApp's Terms of Service ("WhatsApp Terms") by accessing and using WhatsApp. In relevant part, the WhatsApp Terms required Defendants to submit to the personal jurisdiction of this Court.

13. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b), as the threatened and actual harm to WhatsApp and Facebook occurred in this District.

14. Pursuant to Civil L.R. 3-2(d), this case may be assigned to either the San Francisco or Oakland division because WhatsApp and Facebook are located in San Mateo County.

FACTUAL ALLEGATIONS

A. Background on Facebook

15. Facebook is a social networking website and mobile application that enables its users to create their own personal profiles and connect with each other on their personal computers and mobile devices. As of June 2019, Facebook daily active users averaged 1.59 billion and monthly active users averaged 2.41 billion.

16. In October 2014, Facebook acquired WhatsApp. At all times relevant to this action, Facebook has served as WhatsApp's service provider, which entails providing both infrastructure and security for WhatsApp.

B. Background on WhatsApp

1. The WhatsApp Service

17. WhatsApp provides an encrypted communication service available on mobile devices and desktop computers (the "WhatsApp Service"). Approximately 1.5 billion people in 180 countries use the WhatsApp Service. Users must install the WhatsApp app to use the WhatsApp Service.

18. Every type of communication (calls, video calls, chats, group chats, images, videos, voice messages, and file transfers) on the WhatsApp Service is encrypted during its transmission between users. This encryption protocol was designed to ensure that no one other than the intended recipient could read any communication sent using the WhatsApp Service.

2. WhatsApp's Terms of Service

19. Every WhatsApp user must create an account and agree and consent to WhatsApp's Terms (available at https://www.whatsapp.com/legal?eea=0#terms-of-service).

20. The WhatsApp Terms stated that "You must use our Services according to our Terms and policies" and that users agreed to "access and use [WhatsApp's] Services only for legal, authorized, and acceptable purposes."

21. The WhatsApp Terms prohibited using the WhatsApp services in ways that (a) "violate, misappropriate, or infringe the rights of WhatsApp, our users, or others, including privacy;" (b) "are illegal, intimidating, harassing, . . . or instigate or encourage conduct that would be illegal, or otherwise inappropriate;" [or] . . . (e) "involve sending illegal or impermissible communications."

22. The WhatsApp Terms prohibited users from "exploiting [WhatsApp's] Services in impermissible or unauthorized manners, or in ways that burden, impair, or harm us, our Services, systems, our users, or others." The Terms also required users to agree not to: "(a) reverse engineer, alter, modify, create derivative works from, decompile, or extract code from our Services; (b) send, store, or transmit viruses or other harmful computer code through or onto our Services; (c) gain or attempt to gain unauthorized access to our Services or systems; (d) interfere with or disrupt the safety, security, or performance of our Services; [or] . . . (f) collect the information of or about our users in any impermissible or unauthorized manner."

23. The WhatsApp Terms prohibited users not just from personally engaging in the conduct listed above, but also from assisting others in doing so.

C. Background on NSO Group and Pegasus

24. Defendants manufactured, distributed, and operated surveillance technology or "spyware" designed to intercept and extract information and communications from mobile phones and devices. Defendants' products included "Pegasus," a type of spyware known as a remote access trojan. Ex. 10 and 11. According to Defendants, Pegasus and its variants (collectively, "Pegasus") were designed to be remotely installed and enable the remote access and control of information—including calls, messages, and location—on mobile devices using the Android, iOS, and BlackBerry operating systems. *Id.*

25. On information and belief, in order to enable Pegasus' remote installation, Defendants exploited vulnerabilities in operating systems and applications (e.g., CVE-2016-4657) and used other malware delivery methods, like spearphishing messages containing links to malicious code. *Id.*

26. According to media reports and NSO documents, Defendants claimed that Pegasus could be surreptitiously installed on a victim's phone without the victim taking any action, such as

clicking a link or opening a message (known as remote installation).[1] *Id.* Defendants promoted that Pegasus's remote installation feature facilitated infecting victims' phones without using spearphishing messages that could be detected and reported by the victims.

27. According to NSO Group, Pegasus could "remotely and covertly extract valuable intelligence from virtually any mobile device." *Id.* Pegasus was designed, in part, to intercept communications sent to and from a device, including communications over iMessage, Skype, Telegram, WeChat, Facebook Messenger, WhatsApp, and others. *Id.* On information and belief, Pegasus was modular malware, which meant that it could be customized for different purposes, including to intercept communications, capture screenshots, and exfiltrate browser history and contacts from the device. *Id.*

28. Defendants used a network of computers to monitor and update the version of Pegasus implanted on the victims' phones. *Id.* These Defendant-controlled computers relayed malware, commands, and data between a compromised phone, Defendants, and Defendants' customers. This network served as the nerve center through which Defendants supported and controlled their customers' operation and use of Pegasus. In some instances, Defendants limited the number of concurrent devices that their customers could compromise with Pegasus to 25. Ex. 11.

29. Defendants profited by licensing Pegasus and selling support services to their customers, which included Pegasus installation, monitoring, and training. Ex. 10 and 11. Defendants also offered technical support to customers using Pegasus to infect victims' phones, including: (a) technical support by email and phone; and (b) remote troubleshooting by Defendants' engineers through remote desktop software and a virtual private network. *Id.*

[1] *See* Financial Times, "Israel's NSO: the business of spying on your iPhone" (May 14, 2019), *available at* https://www.ft.com/content/7f2f39b2-733e-11e9-bf5c-6eeb837566c5; Vice, "They Got Everything" (September 20, 2018), *available at* https://www.vice.com/en_us/article/qvakb3/inside-nso-group-spyware-demo.

D. Defendants Agreed to the WhatsApp Terms

30. Between January 2018 and May 2019, Defendants created and caused to be created various WhatsApp accounts and agreed to the WhatsApp Terms. Defendants' employees and agents accepted and agreed to be bound by the Terms on behalf of Defendants.

31. At all times relevant to this Complaint, Defendants were bound by the WhatsApp Terms.

E. Defendants Accessed and Used Plaintiffs' Servers Without Authorization and Infected Target Users' Devices With Malware

1. Overview

32. Defendants took a number of steps, using WhatsApp servers and the WhatsApp Service without authorization, to send discrete malware components ("malicious code") to Target Devices. *First*, Defendants set up various computer infrastructure, including WhatsApp accounts and remote servers, used to infect the Target Devices and conceal Defendants' identity and involvement. *Second*, Defendants used and caused to be used WhatsApp accounts to initiate calls through Plaintiffs' servers that were designed to secretly inject malicious code onto Target Devices. *Third*, Defendants caused the malicious code to execute on some of the Target Devices, creating a connection between those Target Devices and computers controlled by Defendants (the "remote servers"). *Fourth*, on information and belief, Defendants caused Target Devices to download and install additional malware—believed to be Pegasus or another remote access trojan developed by Defendants—from the remote servers for the purpose of accessing data and communications on Target Devices.

2. Defendants Set Up Computer Infrastructure Used to Infect the Target Devices

33. Between approximately January 2018 and May 2019, Defendants created WhatsApp accounts that they used and caused to be used to send malicious code to Target Devices in April and May 2019. The accounts were created using telephone numbers registered in different counties, including Cyprus, Israel, Brazil, Indonesia, Sweden, and the Netherlands.

34. Beginning no later than 2019, Defendants leased and caused to be leased servers and internet hosting services in different countries, including the United States, in order to connect the

Target Devices to a network of remote servers intended to distribute malware and relay commands to the Target Devices. This network included proxy servers and relay servers (collectively, "malicious servers"). The malicious servers were owned by Choopa, Quadranet, and Amazon Web Services ("AWS"), among others. The IP address of one of the malicious servers was previously associated with subdomains used by Defendants.

3. Defendants' Unauthorized Access of Plaintiff's Servers

35. On information and belief, Defendants reverse-engineered the WhatsApp app and developed a program to enable them to emulate legitimate WhatsApp network traffic in order to transmit malicious code—undetected—to Target Devices over WhatsApp servers. Defendants' program was sophisticated, and built to exploit specific components of WhatsApp network protocols and code. Network protocols generally define rules that control communications between network computers, including protocols for computers to identify and connect with other computers, as well as formatting rules that specify how data is packaged and transmitted.

36. In order to compromise the Target Devices, Defendants routed and caused to be routed malicious code through Plaintiffs' servers—including Signaling Servers and Relay Servers—concealed within part of the normal network protocol. WhatsApp's Signaling Servers facilitated the initiation of calls between different devices using the WhatsApp Service. WhatsApp's Relay Servers facilitated certain data transmissions over the WhatsApp Service. Defendants were not authorized to use Plaintiffs' servers in this manner.

37. Between approximately April and May 2019, Defendants used and caused to be used, without authorization, WhatsApp Signaling Servers, in an effort to compromise Target Devices. To avoid the technical restrictions built into WhatsApp Signaling Servers, Defendants formatted call initiation messages containing malicious code to appear like a legitimate call and concealed the code within call settings. Disguising the malicious code as call settings enabled Defendants to deliver it to the Target Device and made the malicious code appear as if it originated from WhatsApp Signaling Servers. Once Defendants' calls were delivered to the Target Device, they injected the malicious code into the memory of the Target Device—even when the Target User did not answer the call.

38. For example, on May 9, 2019, Defendants used WhatsApp servers to route malicious code, which masqueraded as a series of legitimate calls and call settings, to a Target Device using telephone number (202) XXX-XXXX. On information and belief, the malicious code concealed within the calls was then installed in the memory of the Target Device.

39. Between April and May 2019, Defendants also used and caused to be used WhatsApp's Relay Servers without authorization to send encrypted data packets designed to activate the malicious code injected into the memory of the Target Devices. When successfully executed, the malicious code caused the Target Device to send a request to one of the malicious servers controlled by Defendants.

40. On information and belief, the malicious servers connected the Target Devices to remote servers hosting Defendants' malware. The malicious code on the Target Devices then downloaded and installed Defendants' malware from those servers.

41. On information and belief, after it was installed, Defendants' malware was designed to give Defendants and their customers access to information and data stored on the Target Devices, including their communications.

42. Between approximately April 29, 2019, and May 10, 2019, Defendants caused their malicious code to be transmitted over WhatsApp servers in an effort to infect approximately 1,400 Target Devices. The Target Users included attorneys, journalists, human rights activists, political dissidents, diplomats, and other senior foreign government officials.

43. The Target Users had WhatsApp numbers with country codes from several countries, including the Kingdom of Bahrain, the United Arab Emirates, and Mexico. According to public reporting, Defendants' clients include, but are not limited to, government agencies in the Kingdom of Bahrain, the United Arab Emirates, and Mexico as well as private entities.[2]

[2] *See* Fast Company, "Israeli cyberweapon targeted the widow of a slain Mexican journalist" (March 20, 2019), *available at* https://www.fastcompany.com/90322618/nso-group-pegasus-cyberweapon-targeted-the-widow-of-a-slain-mexican-journalist; New York Times, "Hacking a Prince, and Emir and a Journalist to Impress a Client" (August 31, 2018), *available at* https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html; The Guardian, "Israeli firm linked to WhatsApp spyware attack faces lawsuit" (May 18, 2019), *available at* https://www.theguardian.com/world/2019/may/18/israeli-firm-nso-group-linked-to-whatsapp-spyware-attack-faces-lawsuit.

44. On or about May 13, 2019, Facebook publicly announced that it had investigated and identified a vulnerability involving the WhatsApp Service (CVE-2019-3568). WhatsApp and Facebook closed the vulnerability, contacted law enforcement, and advised users to update the WhatsApp app.

45. Defendants subsequently complained that WhatsApp had closed the vulnerability. Specifically, NSO Employee 1 stated, "You just closed our biggest remote for cellular . . . It's on the news all over the world."

F. Defendants' Unlawful Acts Have Caused Damage and Loss to WhatsApp and Facebook

46. Defendants' actions and omissions interfered with the WhatsApp Service and burdened Plaintiffs' computer network.

47. Defendants' actions injured Plaintiffs' reputation, public trust, and goodwill.

48. Defendants have caused Plaintiffs damages in excess of $75,000 and in an amount to be proven at trial.

FIRST CAUSE OF ACTION

(Computer Fraud and Abuse Act, 18 U.S.C. § 1030)

49. Plaintiffs reallege and incorporate by reference all preceding paragraphs.

50. At various times between April 29, 2019, and May 10, 2019, Defendants accessed, used, or caused to be accessed or used Plaintiffs' Signaling Servers and Relay Servers without authorization in an effort to compromise approximately 1,400 Target Devices.

51. Plaintiffs' Signaling Servers and Relay Servers and the Target Devices were "computers" as defined by 18 U.S.C. § 1030(e)(1).

52. Plaintiffs' Signaling Servers and Relay Servers and the Target Devices were "protected computers" as defined by 18 U.S.C. § 1030(e)(2)(B) because they are "used in or affecting interstate or foreign commerce or communication."

53. Defendants violated 18 U.S.C. § 1030(a)(2) because they intentionally accessed and caused to be accessed (a) Plaintiffs' computers, and (b) Target Devices, without authorization and, on information and belief, obtained data from the Target Devices.

54. Defendants violated 18 U.S.C. § 1030(a)(4) because they knowingly and with intent to defraud accessed and caused to be accessed (a) Plaintiffs' protected computers and (b) Target Devices without authorization, and by means of such conduct furthered the intended fraud and obtained something of value. Defendants' fraud included falsely agreeing to the WhatsApp Terms, sending unauthorized commands to Plaintiffs' computers and concealing the commands as legitimate network traffic, in order to gain access of the Target Devices without the Target Users' knowledge or consent. As a result of the fraud, Defendants obtained money, customers, remote access and control of the Target Devices, data from the Target Devices, and unauthorized use of the WhatsApp service, the value of which exceeds $5,000.

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

56. Defendants' conduct caused a loss to Plaintiffs and the Target Users in excess of $5,000 during a one-year period.

57. Defendants' actions caused Plaintiffs to incur a loss as defined in 18 U.S.C. § 1030(e)(11), including the expenditure of resources to investigate and remediate Defendants' fraud and unauthorized access. Plaintiffs are entitled to be compensated for losses and damages, and any other amount to be proven at trial.

SECOND CAUSE OF ACTION

(California Comprehensive Computer Data Access and Fraud Act,
California Penal Code § 502)

58. Plaintiffs reallege and incorporate by reference all of the preceding paragraphs.

59. Defendants knowingly accessed and without permission altered and used Plaintiffs' data, computer, computer system, and computer network in order to (a) devise and execute a scheme and artifice to defraud and deceive, and (b) wrongfully control and obtain money, property, and data in violation of California Penal Code § 502(c)(1).

60. Defendants knowingly and without permission used and caused to be used WhatsApp Signaling Servers and Relay Servers, including servers located in California, in violation of California Penal Code § 502(c)(3).

61. Defendants knowingly and without permission provided and assisted in providing a means of accessing Plaintiffs' computers, computer systems, and computer networks, including those located in California, in violation of California Penal Code § 502(c)(6).

62. Defendants knowingly and without permission accessed and caused to be accessed Plaintiffs' computers, computer systems, and computer networks, including those located in California, in violation of California Penal Code § 502(c)(7).

63. Defendants knowingly introduced a computer contaminant into Plaintiffs' computers, computer systems, and computer networks in violation of California Penal Code § 502(c)(8).

64. Defendants' actions caused Plaintiffs to incur losses and damages, including, among other things, the expenditure of resources to investigate and remediate Defendants' conduct, damage to Plaintiffs' reputation, and damage to the relationships and goodwill between Plaintiffs and their users and potential users. Plaintiffs have been damaged in an amount to be proven at trial.

65. Because Plaintiffs suffered damages and a loss as a result of Defendants' actions and continue to suffer damages as result of Defendants' actions, Plaintiffs are entitled to compensatory damages, attorneys' fees, and any other amount of damages to be proven at trial, as well as injunctive relief under California Penal Code §§ 502(e)(1) and (2).

66. Because Defendants willfully violated California Penal Code § 502, and there is clear and convincing evidence that Defendants acted with malice and oppression and committed "fraud" as defined by section 3294 of the Civil Code, Plaintiffs are entitled to punitive and exemplary damages under California Penal Code § 502(e)(4).

THIRD CAUSE OF ACTION

(Breach of Contract)

67. Plaintiffs reallege and incorporate by reference all preceding paragraphs.

68. Access to and use of WhatsApp is governed by the WhatsApp's Terms and related WhatsApp policies.

69. Defendants agreed to and became bound by the WhatsApp's Terms when they used WhatsApp and the WhatsApp Service.

70. WhatsApp and Facebook have performed all conditions, covenants, and promises required of it in accordance with the WhatsApp's Terms.

71. Defendants' violations of the WhatsApp's Terms have directly and proximately caused and continue to cause harm and injury to WhatsApp.

72. When Defendants agreed to and became bound by the WhatsApp Terms, both Plaintiffs and Defendants knew or could have reasonably foreseen that the harm and injury to Plaintiffs was likely to occur in the ordinary course of events as a result of Defendants' breach.

73. Defendants' actions caused Plaintiffs to incur losses and other economic damages, including, among other things, the expenditure of resources to investigate and remediate Defendants' conduct, damage to Plaintiffs' reputation, and damage to the relationships and goodwill between Plaintiffs and their users and potential users. Plaintiffs have been damaged in an amount to be proven at trial, and in excess of $75,000.

FOURTH CAUSE OF ACTION

(Trespass to Chattels)

74. Plaintiffs reallege and incorporate by reference all of the preceding paragraphs.

75. At all times mentioned in this Complaint, Plaintiffs had legal title to and actual possession of their computer systems.

76. Defendants intentionally and without authorization interfered with Plaintiffs' possessory interest in their computer systems, including by accessing and using Plaintiffs' servers to transmit malicious code for the purpose of unlawfully compromising Target Users' devices, all without authorization from Plaintiffs and Target Users.

77. Defendants' access to Plaintiffs' computer systems exceeded the scope of the conditional access that Plaintiffs grant to legitimate users of the WhatsApp Service.

78. Defendants' actions caused Plaintiffs to incur losses and other economic damages, including, among other things, the expenditure of resources to investigate and remediate Defendants' conduct, damage to Plaintiffs' reputation, and damage to the relationships and goodwill between Plaintiffs and their users and potential users. Plaintiffs have been damaged in an amount to be proven at trial, and in excess of $75,000.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs request judgment against Defendants as follows:

1. That the Court enter judgment against Defendants that Defendants have:

   a. Violated the Computer Fraud and Abuse Act, in violation of 18 U.S.C. § 1030;

   b. Violated the California Comprehensive Computer Data Access and Fraud Act, in violation California Penal Code § 502;

   c. Breached their contracts with WhatsApp in violation of California law;

   d. Wrongfully trespassed on Plaintiffs' property in violation of California law.

2. That the Court enter a permanent injunction enjoining and restraining Defendants and their agents, servants, employees, successors, and assigns, and all other persons acting in concert with or conspiracy with any of them or who are affiliated with Defendants from:

   a. Accessing or attempting to access WhatsApp's and Facebook's service, platform, and computer systems;

   b. Creating or maintaining any WhatsApp or Facebook account;

   c. Engaging in any activity that disrupts, diminishes the quality of, interferes with the performance of, or impairs the functionality of Plaintiffs' service, platform, and computer systems; and

   d. Engaging in any activity, or facilitating others to do the same, that violates WhatsApp's or Facebook's Terms;

3. That WhatsApp and Facebook be awarded damages, including, but not limited to, compensatory, statutory, and punitive damages, as permitted by law and in such amounts to be proven at trial.

4. That WhatsApp and Facebook be awarded their reasonable costs, including reasonable attorneys' fees.

5. That WhatsApp and Facebook be awarded pre- and post-judgment interest as allowed by law.

6. That the Court grant all such other and further relief as the Court may deem just and proper.

PLAINTIFFS RESPECTFULLY DEMAND A JURY TRIAL.

Dated: October 29, 2019

Respectively submitted,

COOLEY LLP

/s/ Travis LeBlanc

Travis LeBlanc
Daniel J. Grooms
Joseph D. Mornin

Attorneys for Plaintiffs
WHATSAPP INC. and FACEBOOK, INC.

Platform Enforcement and Litigation
Facebook, Inc.
Jessica Romero
Tyler Smith
Michael Chmelar
Bridget Freeman

EXHIBIT 1

Ministry of Justice **[emblem]** **Registrar of Companies**

State of Israel
Companies Law, 5760-1999

Company Incorporation Certificate

This is to certify that

N.S.O. GROUP TECHNOLOGIES LTD
[bilingual text]

got incorporated and registered according to the Companies Law as a Limited Liability Company

25/01/2010
10th of Sh'vat, 5770

Company no. 514395409

[stamp:]
Ministry of Justice
Registrar of Companies
[emblem:] State of Israel
[signature]
Einat Messika, Adv.
Registrar of Companies

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

[emblem:] State of Israel

Ministry of Justice

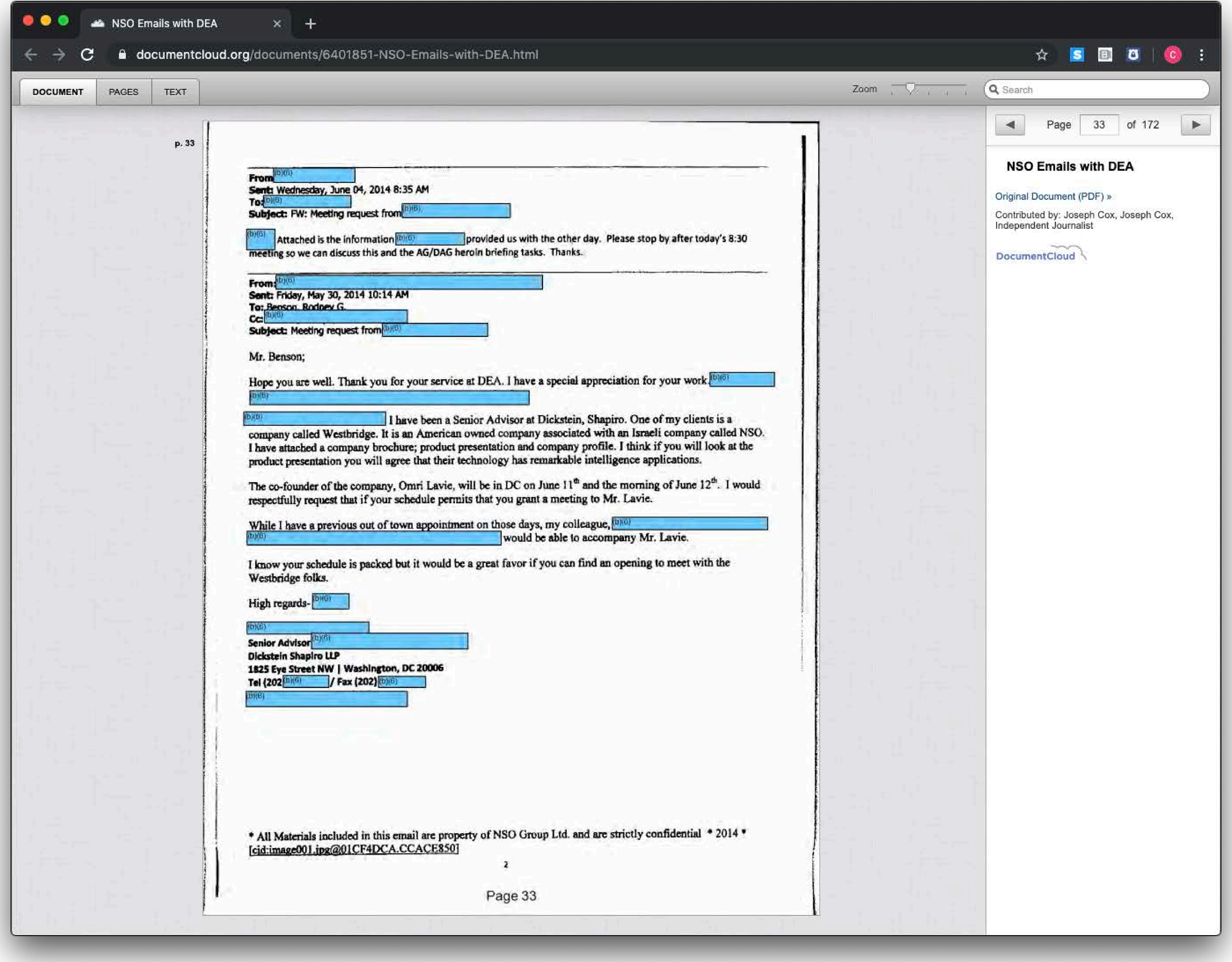
This document is a copy scanned in its entirety on the indicated day and hour, via trusted digital scanning of the document found in the file, in accordance to the inspection regulation at the Ministry of Justice.

Signed by
Ministry of Justice (institutional signature).

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

EXHIBIT 2

09/25/2019 - Screenshot from https://www.documentcloud.org/documents/6401851-NSO-Emails-with-DEA.html


NSO Emails with DEA
documentcloud.org/documents/6401851-NSO-Emails-with-DEA.html
DOCUMENT
PAGES
TEXT
Zoom
Search
p. 33
Page 33 of 172
NSO Emails with DEA
Original Document (PDF) »
Contributed by: Joseph Cox, Joseph Cox, Independent Journalist
DocumentCloud

From (b)(6)
Sent: Wednesday, June 04, 2014 8:35 AM
To: (b)(6)
Subject: FW: Meeting request from (b)(6)

(b)(6) Attached is the information (b)(6) provided us with the other day. Please stop by after today's 8:30 meeting so we can discuss this and the AG/DAG heroin briefing tasks. Thanks.

From: (b)(6)
Sent: Friday, May 30, 2014 10:14 AM
To: Benson, Rodney G.
Cc: (b)(6)
Subject: Meeting request from (b)(6)

Mr. Benson;

Hope you are well. Thank you for your service at DEA. I have a special appreciation for your work. (b)(6) (b)(6)

(b)(6) I have been a Senior Advisor at Dickstein, Shapiro. One of my clients is a company called Westbridge. It is an American owned company associated with an Israeli company called NSO. I have attached a company brochure; product presentation and company profile. I think if you will look at the product presentation you will agree that their technology has remarkable intelligence applications.

The co-founder of the company, Omri Lavie, will be in DC on June 11th and the morning of June 12th. I would respectfully request that if your schedule permits that you grant a meeting to Mr. Lavie.

While I have a previous out of town appointment on those days, my colleague, (b)(6) (b)(6) would be able to accompany Mr. Lavie.

I know your schedule is packed but it would be a great favor if you can find an opening to meet with the Westbridge folks.

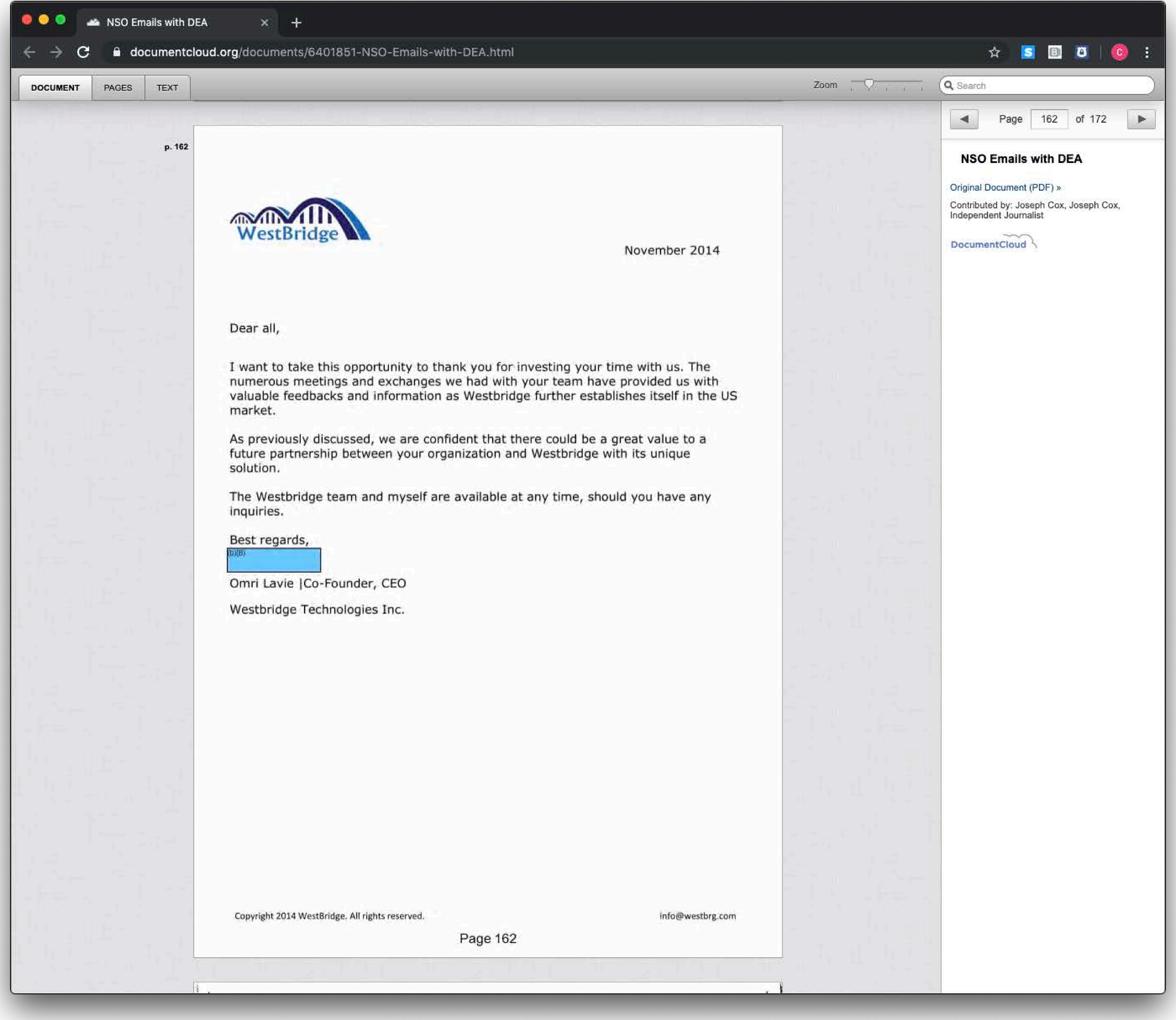
High regards- (b)(6)

(b)(6)
Senior Advisor (b)(6)
Dickstein Shapiro LLP
1825 Eye Street NW | Washington, DC 20006
Tel (202 (b)(6) **/ Fax (202)** (b)(6)
(b)(6)

* All Materials included in this email are property of NSO Group Ltd. and are strictly confidential * 2014 *
[cid:image001.jpg@01CF4DCA.CCACE850]

EXHIBIT 3

09/25/2019 - Screenshot from https://www.documentcloud.org/documents/6401851-NSO-Emails-with-DEA.html


NSO Emails with DEA
documentcloud.org/documents/6401851-NSO-Emails-with-DEA.html
DOCUMENT
PAGES
TEXT
Zoom
Search
Page 162 of 172
NSO Emails with DEA
Original Document (PDF) »
Contributed by: Joseph Cox, Joseph Cox, Independent Journalist
DocumentCloud
p. 162

WestBridge

November 2014

Dear all,

I want to take this opportunity to thank you for investing your time with us. The numerous meetings and exchanges we had with your team have provided us with valuable feedbacks and information as Westbridge further establishes itself in the US market.

As previously discussed, we are confident that there could be a great value to a future partnership between your organization and Westbridge with its unique solution.

The Westbridge team and myself are available at any time, should you have any inquiries.

Best regards,

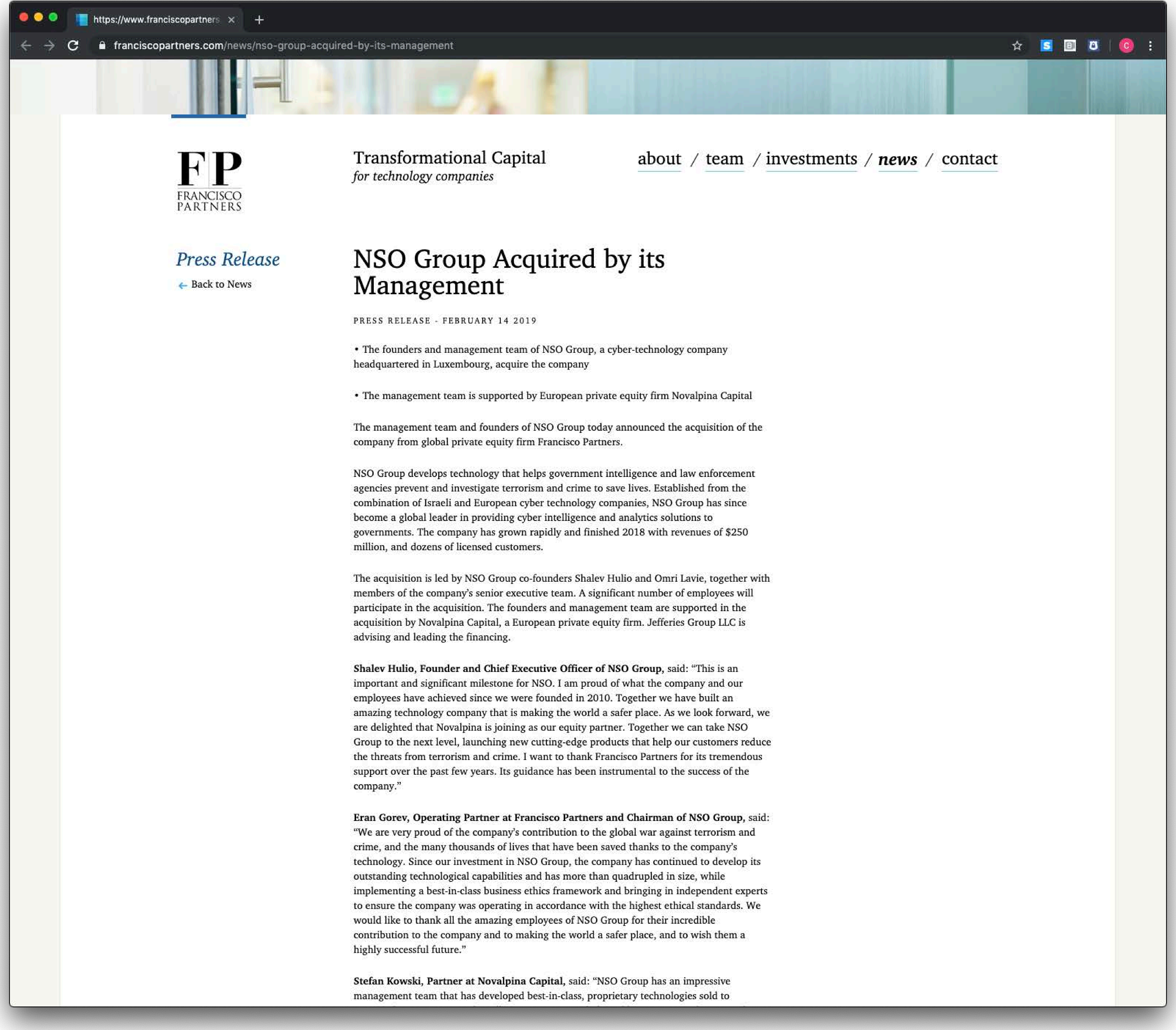
(b)(6)

Omri Lavie |Co-Founder, CEO

Westbridge Technologies Inc.

EXHIBIT 4

09/23/2019 - Screenshot of https://www.franciscopartners.com/news/nso-group-acquired-by-its-management


https://www.franciscopartners
franciscopartners.com/news/nso-group-acquired-by-its-management
FP FRANCISCO PARTNERS
Transformational Capital
for technology companies
about / team / investments / news / contact

Press Release

Back to News

NSO Group Acquired by its Management

PRESS RELEASE - FEBRUARY 14 2019

- The founders and management team of NSO Group, a cyber-technology company headquartered in Luxembourg, acquire the company

- The management team is supported by European private equity firm Novalpina Capital

The management team and founders of NSO Group today announced the acquisition of the company from global private equity firm Francisco Partners.

NSO Group develops technology that helps government intelligence and law enforcement agencies prevent and investigate terrorism and crime to save lives. Established from the combination of Israeli and European cyber technology companies, NSO Group has since become a global leader in providing cyber intelligence and analytics solutions to governments. The company has grown rapidly and finished 2018 with revenues of $250 million, and dozens of licensed customers.

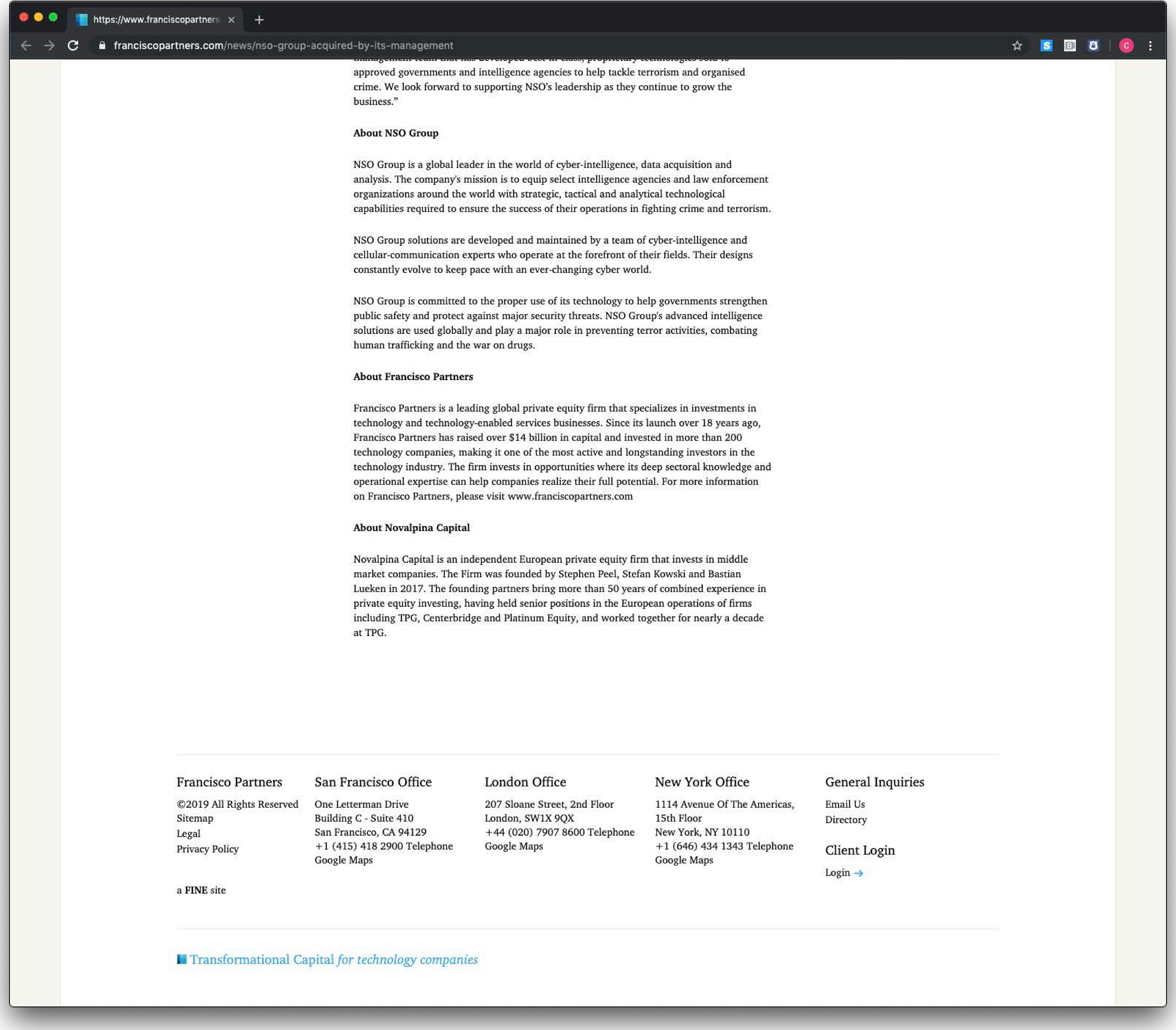
The acquisition is led by NSO Group co-founders Shalev Hulio and Omri Lavie, together with members of the company's senior executive team. A significant number of employees will participate in the acquisition. The founders and management team are supported in the acquisition by Novalpina Capital, a European private equity firm. Jefferies Group LLC is advising and leading the financing.

Shalev Hulio, Founder and Chief Executive Officer of NSO Group, said: "This is an important and significant milestone for NSO. I am proud of what the company and our employees have achieved since we were founded in 2010. Together we have built an amazing technology company that is making the world a safer place. As we look forward, we are delighted that Novalpina is joining as our equity partner. Together we can take NSO Group to the next level, launching new cutting-edge products that help our customers reduce the threats from terrorism and crime. I want to thank Francisco Partners for its tremendous support over the past few years. Its guidance has been instrumental to the success of the company."

Eran Gorev, Operating Partner at Francisco Partners and Chairman of NSO Group, said: "We are very proud of the company's contribution to the global war against terrorism and crime, and the many thousands of lives that have been saved thanks to the company's technology. Since our investment in NSO Group, the company has continued to develop its outstanding technological capabilities and has more than quadrupled in size, while implementing a best-in-class business ethics framework and bringing in independent experts to ensure the company was operating in accordance with the highest ethical standards. We would like to thank all the amazing employees of NSO Group for their incredible contribution to the company and to making the world a safer place, and to wish them a highly successful future."

Stefan Kowski, Partner at Novalpina Capital, said: "NSO Group has an impressive management team that has developed best-in-class, proprietary technologies sold to

09/23/2019 - Screenshot of https://www.franciscopartners.com/news/nso-group-acquired-by-its-management


https://www.franciscopartners
franciscopartners.com/news/nso-group-acquired-by-its-management

management team that has developed best in class, proprietary technologies sold to approved governments and intelligence agencies to help tackle terrorism and organised crime. We look forward to supporting NSO's leadership as they continue to grow the business."

About NSO Group

NSO Group is a global leader in the world of cyber-intelligence, data acquisition and analysis. The company's mission is to equip select intelligence agencies and law enforcement organizations around the world with strategic, tactical and analytical technological capabilities required to ensure the success of their operations in fighting crime and terrorism.

NSO Group solutions are developed and maintained by a team of cyber-intelligence and cellular-communication experts who operate at the forefront of their fields. Their designs constantly evolve to keep pace with an ever-changing cyber world.

NSO Group is committed to the proper use of its technology to help governments strengthen public safety and protect against major security threats. NSO Group's advanced intelligence solutions are used globally and play a major role in preventing terror activities, combating human trafficking and the war on drugs.

About Francisco Partners

Francisco Partners is a leading global private equity firm that specializes in investments in technology and technology-enabled services businesses. Since its launch over 18 years ago, Francisco Partners has raised over $14 billion in capital and invested in more than 200 technology companies, making it one of the most active and longstanding investors in the technology industry. The firm invests in opportunities where its deep sectoral knowledge and operational expertise can help companies realize their full potential. For more information on Francisco Partners, please visit www.franciscopartners.com

About Novalpina Capital

Novalpina Capital is an independent European private equity firm that invests in middle market companies. The Firm was founded by Stephen Peel, Stefan Kowski and Bastian Lueken in 2017. The founding partners bring more than 50 years of combined experience in private equity investing, having held senior positions in the European operations of firms including TPG, Centerbridge and Platinum Equity, and worked together for nearly a decade at TPG.

Francisco Partners
©2019 All Rights Reserved
Sitemap
Legal
Privacy Policy

a **FINE** site

San Francisco Office
One Letterman Drive
Building C - Suite 410
San Francisco, CA 94129
+1 (415) 418 2900 Telephone
Google Maps

London Office
207 Sloane Street, 2nd Floor
London, SW1X 9QX
+44 (020) 7907 8600 Telephone
Google Maps

New York Office
1114 Avenue Of The Americas,
15th Floor
New York, NY 10110
+1 (646) 434 1343 Telephone
Google Maps

General Inquiries
Email Us
Directory

Client Login
Login →

Transformational Capital *for technology companies*

EXHIBIT 5

[emblem:]
State of Israel

State of Israel
Ministry of Justice
Corporations Authority
Registrar of Companies

[logo:]
[text cut off]
[barcode:] 17042-905

Private Company Annual Report

(Section 141 of the Companies Law 5759-1999 (hereinafter: "the Law"))

The data can be typed in or filled out in clear handwriting without using black ink.

Company name NSO Group Technologies Ltd.	**Company number** 514395409	**Address of the registered office**[1] 22 Galgalei Haplada, Hertsliya, Israel 4672222

Telephone	**Company Email (if any)**
The report is updated as of (state the date of signing the report in order to submit it to the Registrar of Companies) [hw:] *7/1/19*	**Annual meeting was conducted on the day**[2] 7.1.2019

Share Capital Distribution

Total registered capital of the company 10,000	**Share name and its set value (for shares with set value)** Ordinary, set value – 0.01 Ordinary A, set value – 0.01 Preferred A, set value – 0.01	**Share type** Ordinary Ordinary A Preferred A
Number of shares in the registered capital Ordinary – 548,940 Ordinary A – 26,290 Preferred A – 424,770	**Number of allotted shares** Ordinary – 185,716 Ordinary A – 8,936 Preferred A – 295,170	**Share value** 0.01

Shareholders and their shares

Shareholder name Q Cyber Technologies Ltd **Type of shares** Ordinary Ordinary A Preferred A	**ID number**[3] 514971522 **Number of shares** 118,263 8,936 295,170	**Address (city, street, house no., zip code)** 22 Galgalei Haplada, Hertsliya, Israel Zip Code 4672222 **Unpaid amount in exchange for the shares**
Shareholder name NSO Group Technologies Ltd. **Type of shares** Ordinary	**ID number**[3] 514395409 **Number of shares** 67,453	**Address (city, street, house no., zip code)** 22 Galgalei Haplada, Hertsliya, Israel Zip Code 4672222 **Unpaid amount in exchange for the shares**

[stamp:]
State of Israel
Ministry of Justice, Corporations Authority
Public Service – Jerusalem Region
28-02-2019
RECEIVED

[1] Listing a P.O. Box as the company's address is not enough.

[2] The last date on which the annual meeting was conducted, indicate below in the appropriate place whether the company is exempt from conducting annual meetings according to Section 61 of the Law.

[3] A non-holder of the Israeli ID shall indicate his passport number and the country it was issued in, and in the first report of this person, a copy shall be attached, as stated in Regulation 16 of the Companies Regulations (reporting, registration details and forms), 5760-1999. If the shareholder is a corporation, a registration number of the corporation shall be indicated, and if it is a foreign corporation, the copy of incorporation certificate and the required certificates as stated in Regulation 16, shall be attached in the first report of the corporation.

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

[emblem:]
State of Israel

State of Israel
Ministry of Justice
Corporations Authority
Registrar of Companies

[logo:]
Corporations Authority

Bearer Shares for the period

*** Fill out if bearer shares have been issued before 17.09.2016, and the update has not been performed as stated below:**
In accordance with the Amendment no. 28 to the Companies Law 5759-1999, which came into force on 17.09.2016, bearer shares can be no longer issued. A holder of bearer shares issued on the eve of the law coming into force shall be entitled to return the banknote to the company, and the company shall cancel it and issue a share for him that is registered in the Registry of Shareholders of the Company. A bearer share that is not returned as stated shall become a frozen share, as stated in Section 308 of the Law, and it shall not grant him rights until the date stated on the share, which will be recorded in the Registry of Shareholders of the Company.

Total bearer shares for the period	No. of shares in each note	Note no.

Details of active directors

Director name	**ID number**	**Starting date as a director (year, month, day)**
Q Cyber Technologies Ltd	514971522	19/3/2014
Address (city, street, house no., zip code) 22 Galgalei Haplada, Hertsliya, Israel 4672222		

Details of directors who stopped their activity (since the date of the previous annual report)

Director name	**ID number**	**End date as a director (year, month, day)**
Director name	**ID number**	**End date as a director (year, month, day)**
Director name	**ID number**	**End date as a director (year, month, day)**
Director name	**ID number**	**End date as a director (year, month, day)**

Mark the appropriate option with X:

No change has occurred in the details that were reported regarding the foreign directors according to Regulation 16 from the mentioned regulations.

Change has occurred in the details that were reported regarding the foreign directors, and the documents required under Regulation 16 have been attached to the annual report.

Authorized party to report to the registrar on behalf of the company, according to Section 39 of the Law

Filling out the details of the authorized party to report according to Section 39 in this Form will allow the party whose details are entered here to relay updates about the company in a digital manner.
For more information, see: http://www.justice.gov.il/Units/RasutHataagidim/units/RashamHachvarot/TfasimNew/Pages/Online.aspx

Full name	**ID number**	**Position in the company**
[hw:] [illegible] *Idisis*	*032063521*	*Financial director*

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

EXHIBIT 6

[emblem:]
State of Israel

State of Israel
Ministry of Justice – Corporations Authority
Registrar of Companies and Partnerships

[logo:]
Corporations Authority

Company Incorporation Certificate

This is to certify that the company:

L.E.G.D. COMPANY LTD

[bilingual text]

whose number is 514971522

got incorporated and registered on 02/12/2013 - 29th of Kislev 5774,
according to the Companies Law, 5760-1999, as a Limited Liability Company.

Issued in Jerusalem on:

02/12/2013
29th of Kislev 5774

[signature]
Zohar Horan
Corporations Authority
Registrar of Companies and Partnerships

[stamp:]
Ministry of Justice
Registrar of Companies
and Partnerships
[emblem:] State of Israel

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

[emblem:] State of Israel

Ministry of Justice

This document is a copy scanned in its entirety on the indicated day and hour, via trusted digital scanning of the document found in the file, in accordance to the inspection regulation at the Ministry of Justice.

Signed by
Ministry of Justice (institutional signature).

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

EXHIBIT 7

[stamp:]
Document Start

[emblem:]
State of Israel

State of Israel
Ministry of Justice – Corporations Authority
Registrar of Companies and Partnerships

[logo:]
Corporations Authority

Company Name Change Certificate

This is to certify that the company

L.E.G.D. COMPANY LTD

[bilingual text]

whose number is 514971522

has changed its name, and it shall be called from now on

Q CYBER TECHNOLOGIES LTD

[bilingual text]

Issued in Jerusalem on

29/05/2016
21st of Iyyar, 5776

[stamp:]
[emblem:] State of Israel
Ministry of Justice
Registrar of Companies and Partnerships

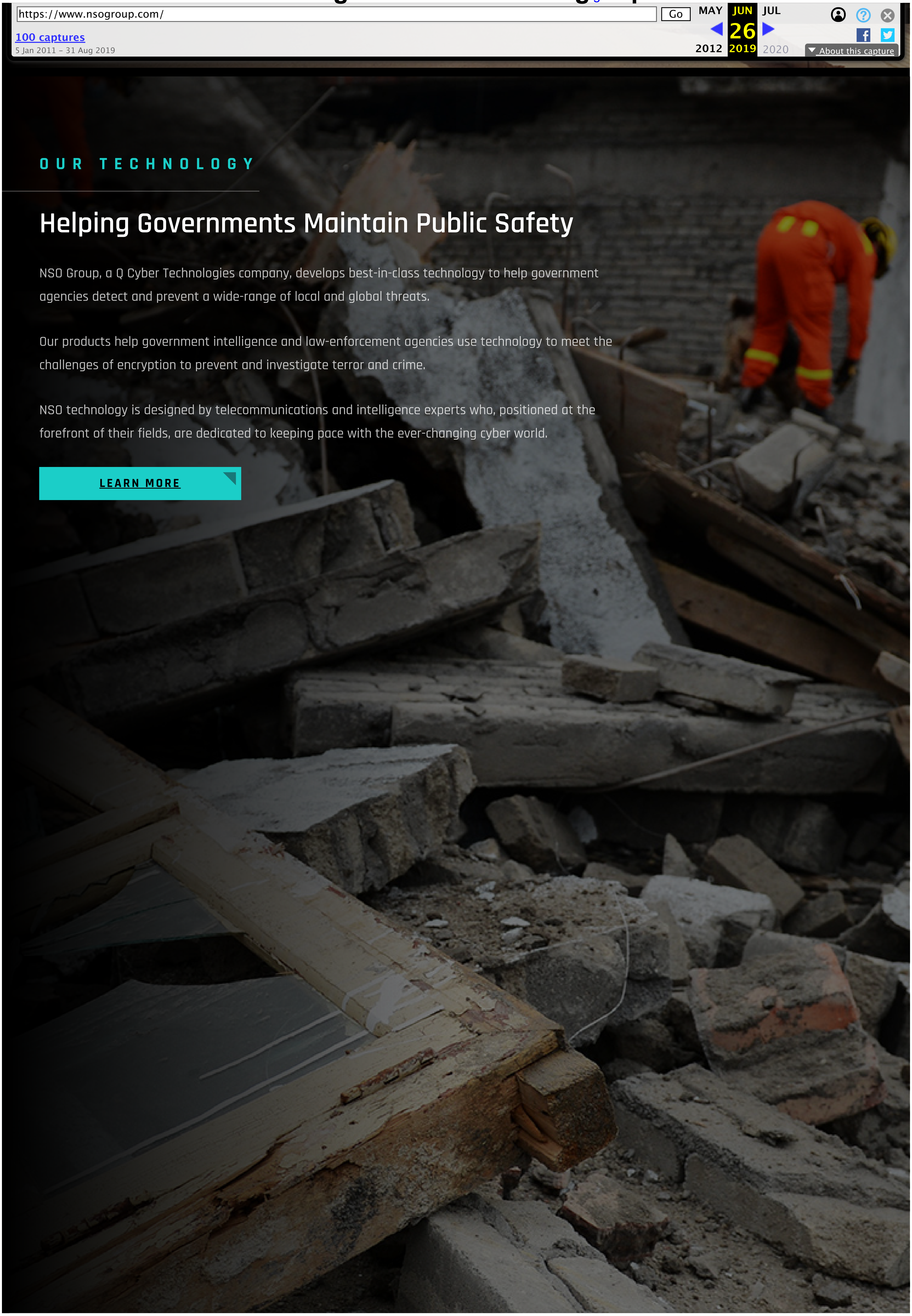
[signature]
Eyal Globus, Adv.
Registrar of Companies and Partnerships
Head of Corporations Authority

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

Issued by Eyal Goldring

EXHIBIT 8

06/26/19 - web.archive.org screenshot of nsogroup.com



https://www.nsogroup.com/ Go

100 captures

5 Jan 2011 – 31 Aug 2019

MAY JUN JUL

2012 26 2019 2020

About this capture

OUR TECHNOLOGY

Helping Governments Maintain Public Safety

NSO Group, a Q Cyber Technologies company, develops best-in-class technology to help government agencies detect and prevent a wide-range of local and global threats.

Our products help government intelligence and law-enforcement agencies use technology to meet the challenges of encryption to prevent and investigate terror and crime.

NSO technology is designed by telecommunications and intelligence experts who, positioned at the forefront of their fields, are dedicated to keeping pace with the ever-changing cyber world.

LEARN MORE

EXHIBIT 9

[emblem:]
State of Israel

State of Israel
Ministry of Justice
Corporations Authority
Registrar of Companies

[logo:]
[text cut off]
[barcode:] 17903-560

Private Company Annual Report

(Section 141 of the Companies Law 5759-1999 (hereinafter: "the Law"))

The data can be typed in or filled out in clear handwriting without using black ink.

Company name Q Cyber Technologies Ltd	**Company number** 514971522	**Address of the registered office**[1] 22 Galgalei Haplada, Hertsliya, Israel 4672222

Telephone	**Company Email (if any)**
The report is updated as of (state the date of signing the report in order to submit it to the Registrar of Companies) [hw:] *16/6/19*	**Annual meeting was conducted on the day**[2] 7.1.2019

Share Capital Distribution

Total registered capital of the company 100,000	**Share name and its set value (for shares with set value)** Ordinary, set value – 0.01	**Share type** Ordinary
Number of shares in the registered capital Ordinary – 10,000,000	**Number of allotted shares** Ordinary – 100,000	**Share value** 0.01

Shareholders and their shares

Shareholder name OSY TECHNOLOGIES S.A.R.L.	**ID number**[3] B184226	**Address (city, street, house no., zip code)** Luxembourg
Type of shares Ordinary	**Number of shares** 100,000	**Unpaid amount in exchange for the shares**

Bearer Shares for the period*

*** Fill out if bearer shares have been issued before 17.09.2016, and the update has not been performed as stated below:**
In accordance with the Amendment no. 28 to the Companies Law 5759-1999, which came into force on 17.09.2016, bearer shares can be no longer issued. A holder of bearer shares issued on the eve of the law coming into force shall be entitled to return the banknote to the company, and the company shall cancel it and issue a share for him that is registered in the Registry of Shareholders of the Company. A bearer share that is not returned as stated shall become a frozen share, as stated in Section 308 of the Law, and it shall not grant him rights until the date stated on the share, which will be recorded in the Registry of Shareholders of the Company.

[stamp:]
State of Israel
Ministry of Justice Corporations Authority
Public Service – Jerusalem Region
17-06-2019
RECEIVED

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

[1] Listing a P.O. Box as the company's address is not enough.
[2] The last date on which the annual meeting was conducted. Indicate below in the appropriate place whether the company is exempt from conducting annual meetings according to Section 61 of the Law.
[3] A non-holder of the Israeli ID shall indicate his passport number and the country it was issued in, and in the first report of this person, a copy shall be attached, as stated in Regulation 16 of the Companies Regulations (reporting, registration details and forms), 5760-1999. If the shareholder is a corporation, a registration number of the corporation shall be indicated, and if it is a foreign corporation, the copy of incorporation certificate and the required certificates as stated in Regulation 16, shall be attached in the first report of the corporation.

Total bearer shares for the period	No. of shares in each note	Note no.

Details of active directors

Director name OSY TECHNOLOGIES S.A.R.L.	ID number B184226	Starting date as a director (year, month, day) 17/3/2014
Address (city, street, house no., zip code) Luxembourg		

Details of directors who stopped their activity (since the date of the previous annual report)

Director name	**ID number**	**End date as a director (year, month, day)**
Director name	**ID number**	**End date as a director (year, month, day)**
Director name	**ID number**	**End date as a director (year, month, day)**
Director name	**ID number**	**End date as a director (year, month, day)**

Mark the appropriate option with X:

No change has occurred in the details that were reported regarding the foreign directors according to Regulation 16 from the mentioned regulations.

Change has occurred in the details that were reported regarding the foreign directors, and the documents required under Regulation 16 have been attached to the annual report.

Authorized party to report to the registrar on behalf of the company, according to Section 39 of the Law

Filling out the details of the authorized party to report according to Section 39 in this Form will allow the party whose details are entered here to relay updates about the company in a digital manner.
For more information, see: http://www.justice.gov.il/Units/RasutHataagidim/units/RashamHachvarot/TfasimNew/Pages/Online.aspx

Full name	ID number	Position in the company
Yifa Idisis	032063521	Financial director

Fulfillment of the instructions of Section 171 (C) of the Law

The Board of Directors has approved the financial reports __ (mark **X** if done).

Fulfillment of the instructions of Section 173 of the Law – (mark the appropriate option with **X**)

The financial documents have been presented at the last annual meeting as required.

If the company is not required to conduct annual meetings according to Section 61 (A) of the Law, indicate whether the financial reports have been sent to the shareholders according to Section 61 (A) of the Law.

The company is not required to submit financial reports at the annual meeting, as stated in Section 172 (G) of the Law.

Controlling accountant (mark the appropriate option with **X**).

The company has a controlling accountant, as stated in Section 154 of the Law.

[stamp:]
[logo]
Corporations Authority
A confirmation that this document has been signed electronically, it is a copy of the document (original or copy) that is in the file of the Corporations Authority on the day of the signature

EXHIBIT 10

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:

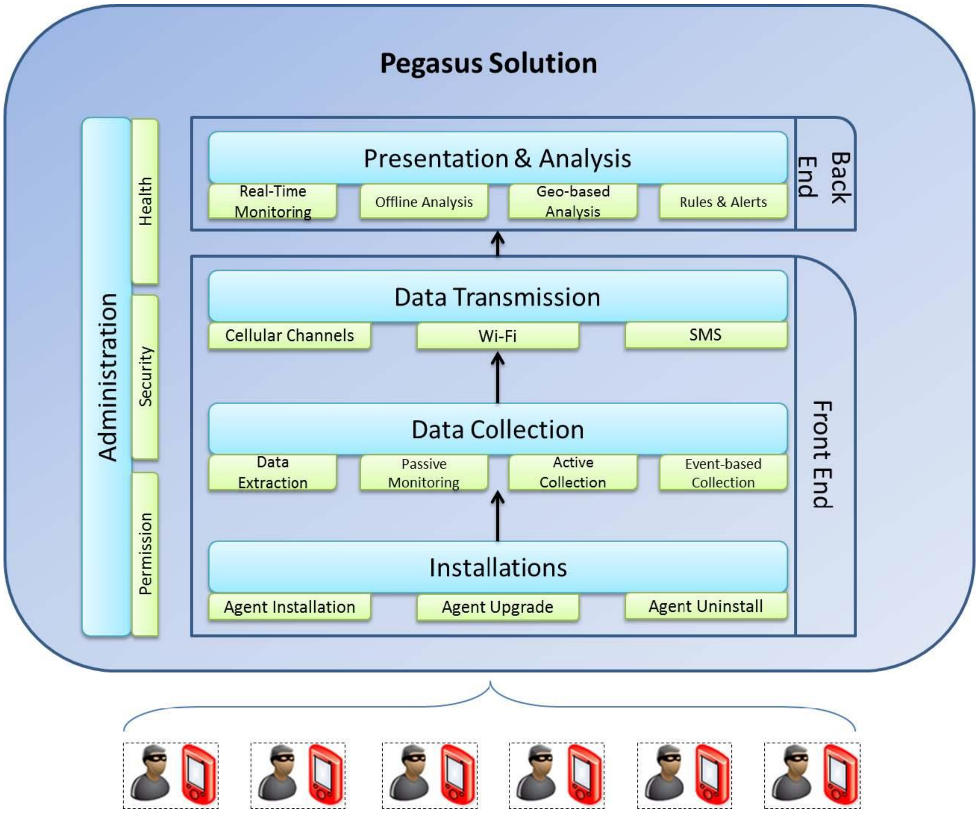
– Permission: The permissions mechanism allows the system administrator to manage the different users of the system. Provide each one of them the right access level only to the data they are allowed to. This allows to define groups in the organization that handle only one or more topics and other groups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

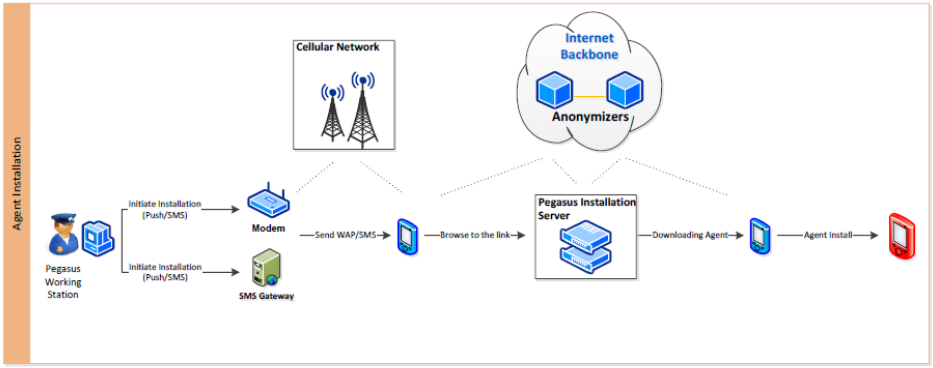
- Tactical Network Element: The Pegasus agent can be silently injected once the number is acquired using tactical network element such as Base Transceiver Station (BTS). The Pegasus solution leverages the capabilities of such tactical tools to perform a remote injection and installation of the agent. 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.

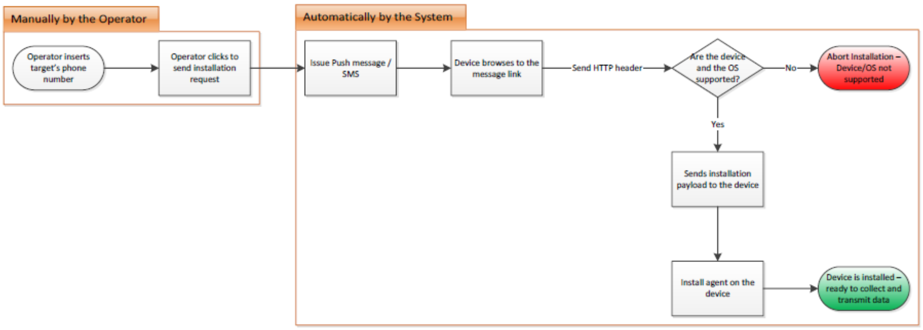
Figure 2: Agent Installation Flow



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.

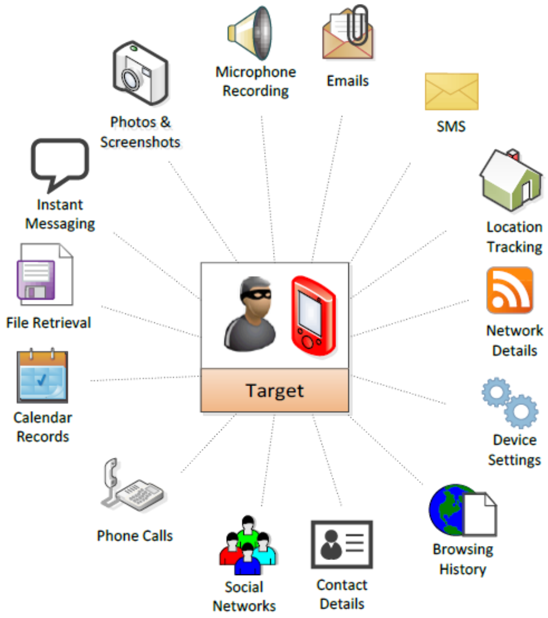
Data Collection

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.

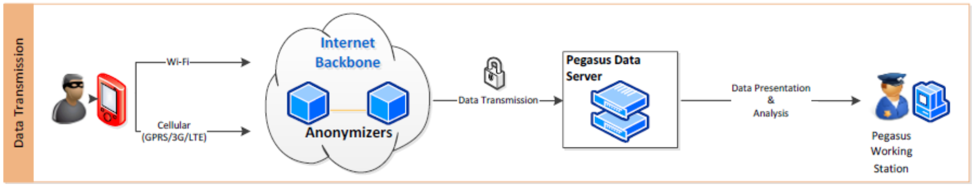
When no data channels are available, and no indication for communication is coming back from the device, the user can request the device will communicate and/or send some crucial data using text messages (SMS).

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.

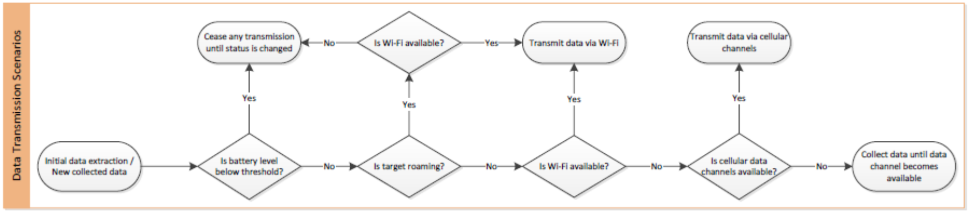
The Pegasus system data transmission process is shown in Figure 5.

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

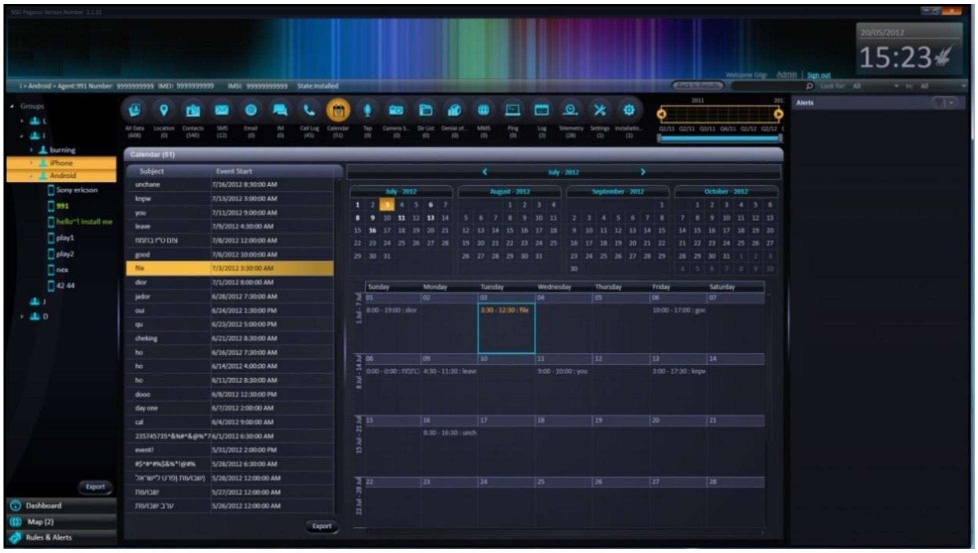
The collected data is organized by groups of interest (e.g., drugs group A, terror group B, etc.) and each group consists of targets. Each target consists of several devices which some have installed agents on them.

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



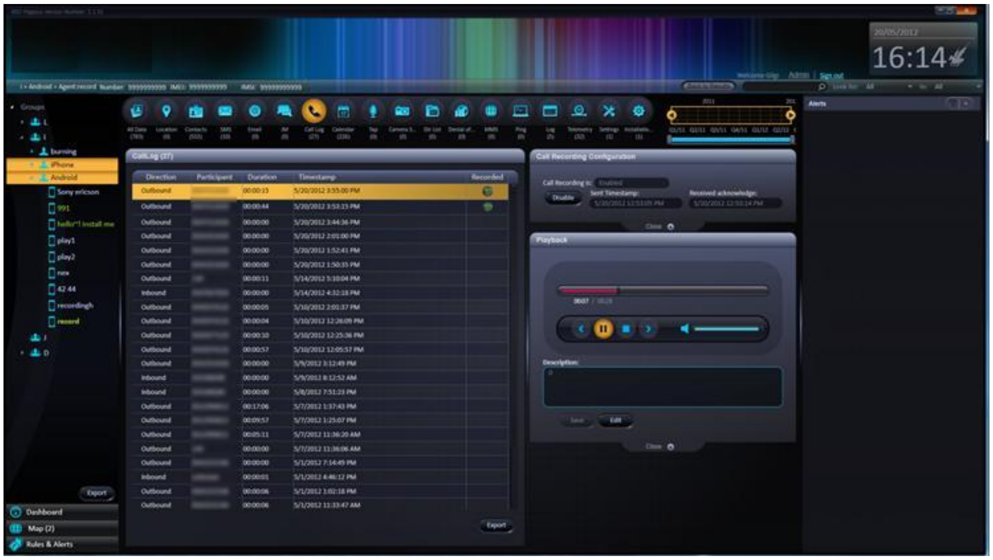
Number: 9999999999 IMEI: 9999999999 IMSI: 99999999999 State:Installed

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

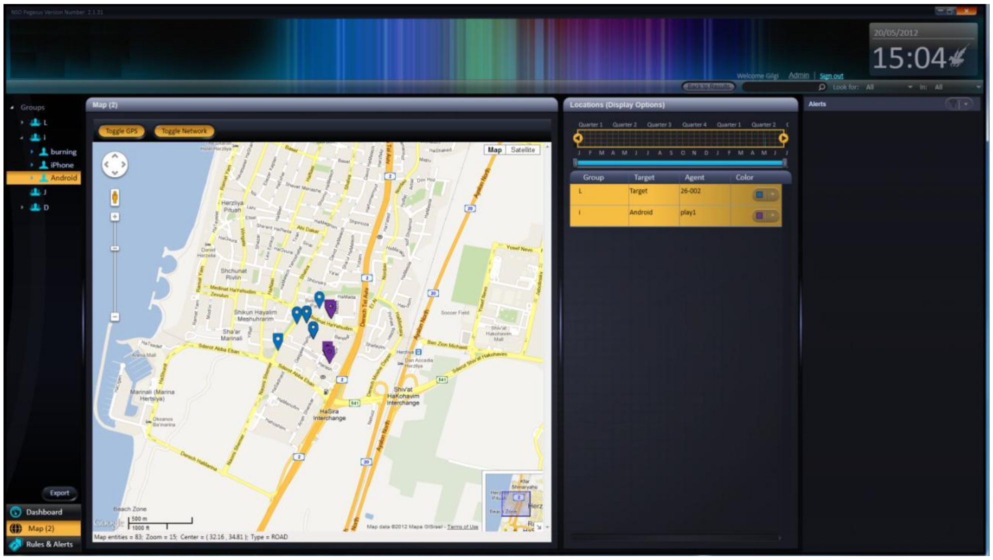


Call Log (27)

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



Locations (Display Options)

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.

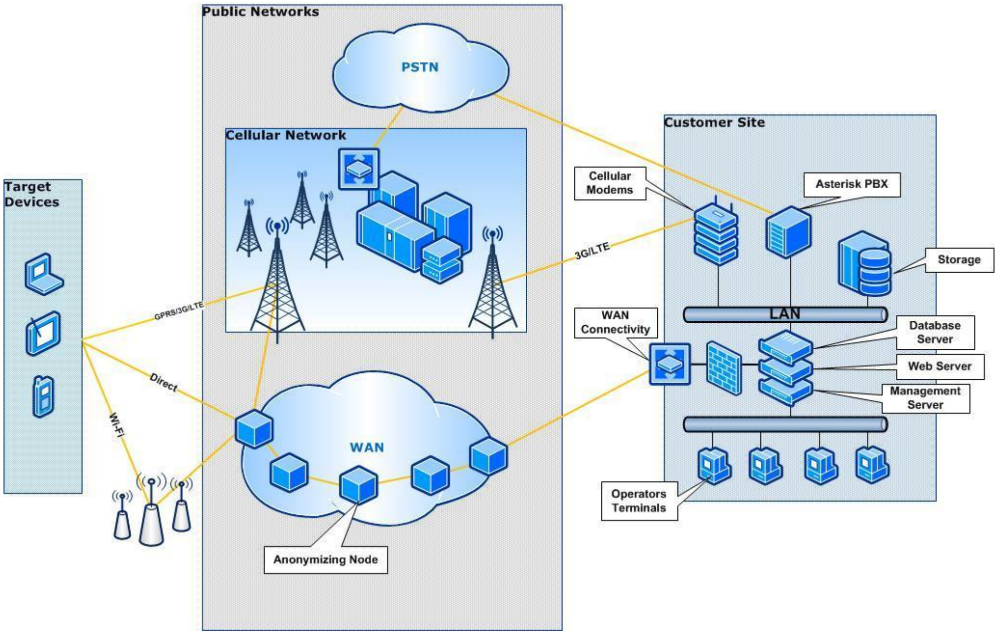
[4] In some cases, uninstall can result in device reboot. If reboot takes place, it happens once agent removal is done. The device comes up clean with no agent installed.

[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

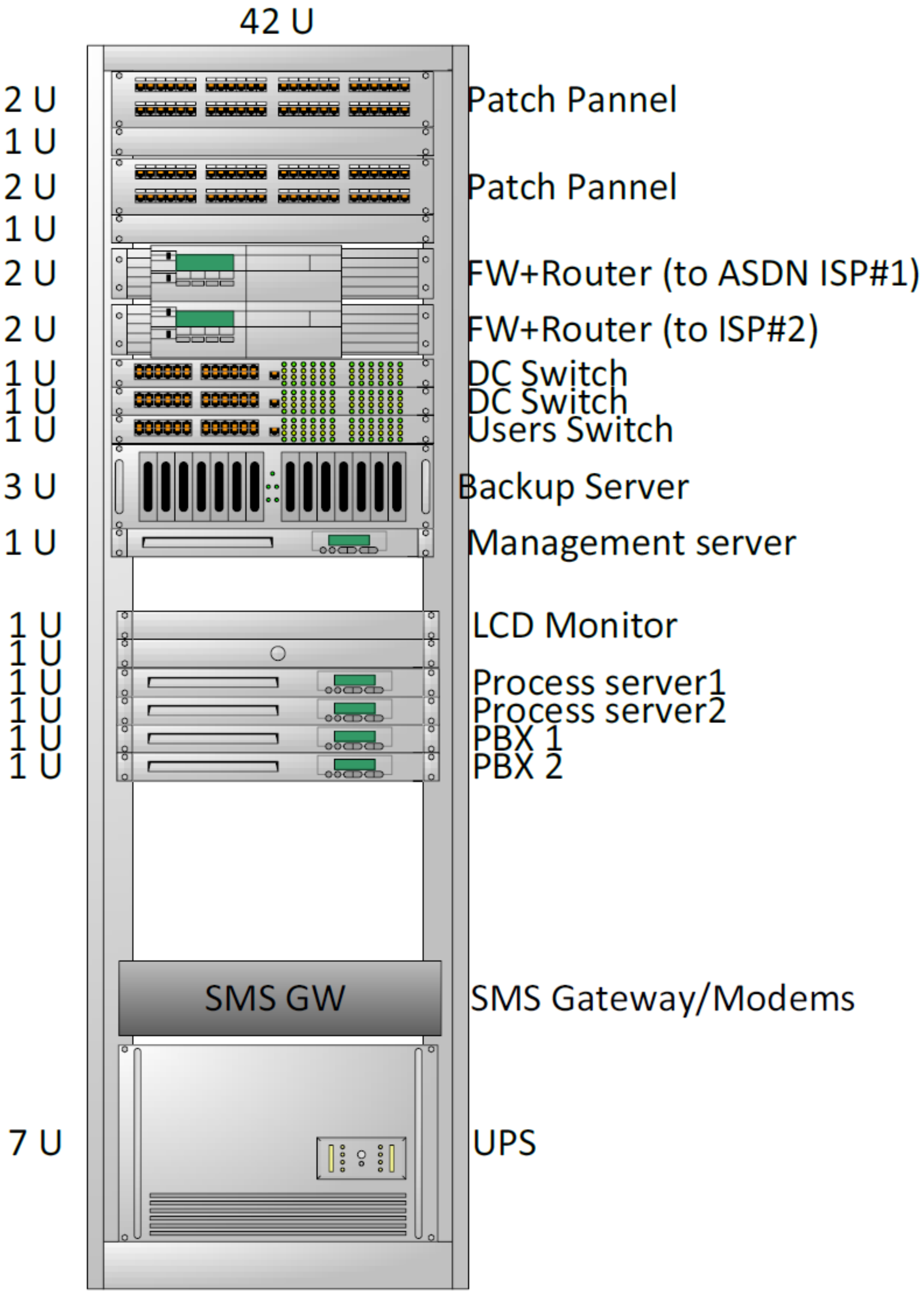
System Hardware

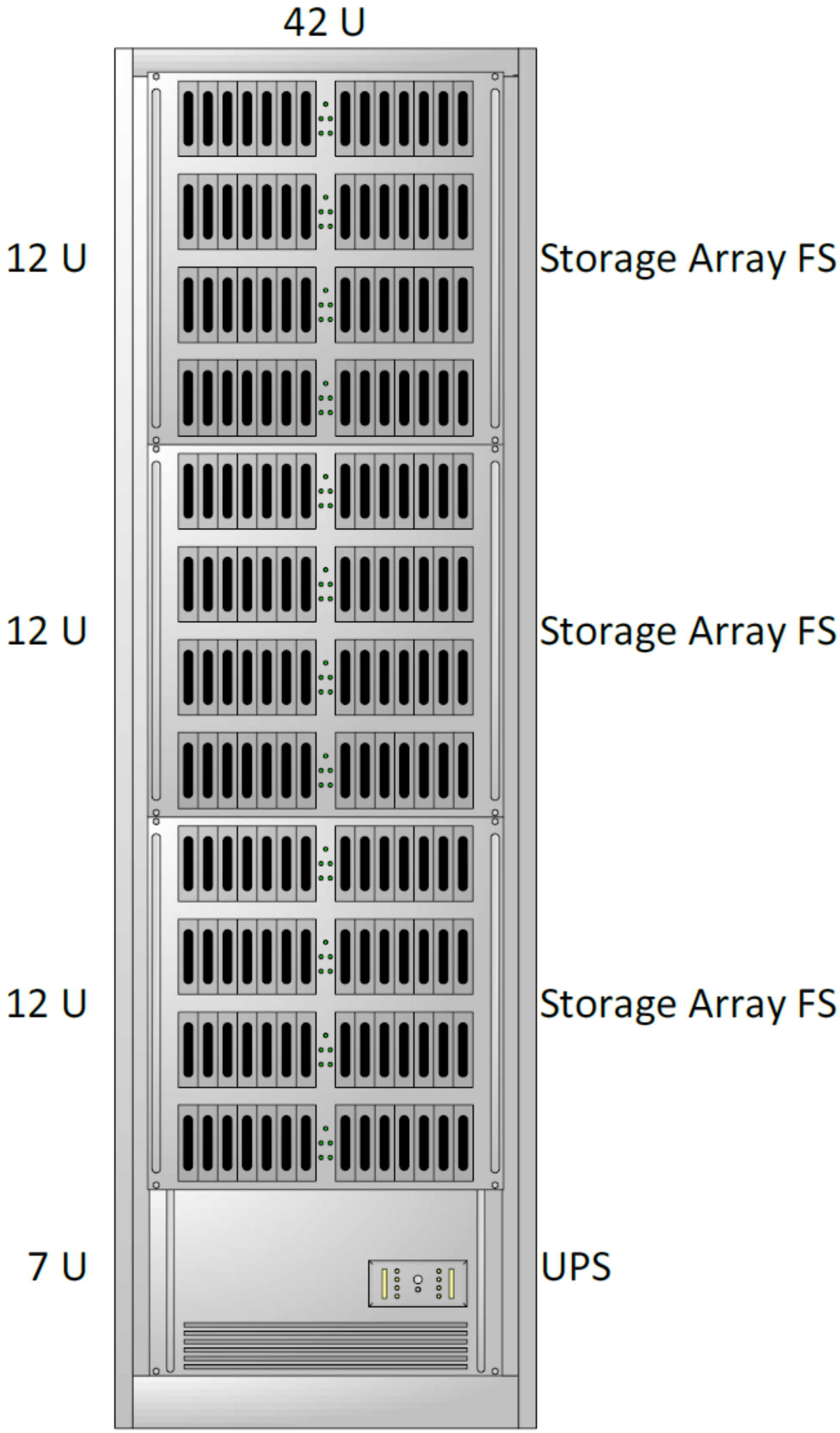
To fully support the system infrastructure, the following hardware is required:

- 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

Week Phase	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Phase 1 - Preparations	ATP req.	Equipment acquisition													
		System Integration													
			Local Networks Adjustments												
Phase 2 - Implementation						System Testing									
								HW Installation							
									Device Porting Process						
Phase 3 – Training & Completion												System Training			
														Customer ATP	

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

EXHIBIT 11

"ID A" dtd 16-01-18

129

79

CONTRACT

IDL × MCA

EXHS

21-2-19

B 123

80

AGREEMENT

This Agreement (the "**Agreement**") is entered into on December 17th, 2015 (the "**Effective Date**") between Infraloks Development Limited, a company incorporated under the laws of the Republic of Ghana (company registration number CA-66,115), having its registered offices at HSE number 1 plot 50, 7th Avenue Extension, North Ridge ACCRA, P.O. Box 30712 KIA, ACCRA (the "**Company**") and the National Communication Authority of the Republic of Ghana (the "**End-User**").

Whereas, the Company is engaged in the business of reselling and supplying cyber intelligence solutions developed, integrated and supplied by the NSO Group Technologies Ltd. (company registration number 514395409), an Israeli Company, having its registered offices at 9 Hamada St., Herzliya, Israel (the "**System Provider**") which has developed the System (as defined below); and

Whereas, the End-User is interested to purchase from the Company a License (as defined below) to use the System (as defined below), and obtain services related to it, solely for the use of the End-User as further set forth herein, and the Company has agreed to provide a License to use the System and related services to the End-User; and

Whereas, the parties wish to set forth the terms under which such sale and purchase shall be made.

Now, therefore, in consideration of the foregoing premises and the mutual covenants herein contained, and for other good and valuable consideration, the parties agree as follows:

1. <u>Definitions and Exhibits</u>.

1.1. In this Agreement, unless the context otherwise requires, terms defined in the preamble and the recitals shall have the same meaning when used elsewhere in this Agreement and the following terms shall have the meanings ascribed thereto below:

"**Agreement**" has the meaning ascribed to it in the preamble.

"**Approval**" has the meaning ascribed to it in Section 5.1.

"**Business Day**" means a day (other than a Friday, Saturday or Sunday) on which banks are generally open in Israel and in the Republic of Ghana for normal business.

"**Certificate**" has the meaning ascribed to it in Section 5.1.

"**Commissioning Notice**" has the meaning ascribed to it in Exhibit B.

"**Company**" has the meaning ascribed to it in the preamble.

"**Confidential Information**" means any information provided by the Company to the and/or the End-User.

"**Deployment**" has the meaning ascribed to it in Exhibit A.

"**Effective Date**" has the meaning ascribed to it in the preamble.

"**End-User**" has the meaning ascribed to it in the preamble.

"**First Installment**" has the meaning ascribed to it in Exhibit B.

"**Force Majeure**" has the meaning ascribed to it in Section 14.

"**Hardware Equipment**" has the meaning ascribed to it in Exhibit A.

"**IMOD**" means the Israeli Ministry of Defense.

"**License**" has the meaning ascribed to it in Section 2.1.

"**Reseller**" N/A.

"**Reseller Representative**" N/A.

"**Reseller Appointment Letter**" N/A.

WT

"**Reseller Appointment Letter**" N/A.

"**End-User Responsibilities**" has the meaning ascribed to it in Section 4.

"**Services**" has the meaning ascribed to it in Exhibit A.

"**SLA**" has the meaning ascribed to in Section 6.2

"**Support Period**" has the meaning ascribed to it in Section 6.1.

"**Support Period Consideration**" has the meaning ascribed to it in Exhibit B.

"**Support Services**" has the meaning ascribed to it in Section 6.

"**System**" has the meaning ascribed to it in Exhibit A.

"**System Consideration**" has the meaning ascribed to it in Exhibit B.

"**System Provider**" has the meaning ascribed to it at the preamble.

"**Training**" has the meaning ascribed to it in,Exhibit A.

"**Warranty**" has the meaning ascribed to it in Exhibit A.

"**Warranty Period**" has the meaning ascribed to it in Exhibit A.

1.2. The following are the exhibits in this Agreement:

Exhibit A – Description of System and Services

Exhibit A-1 – Features and Capabilities

Exhibit A-2 – List of Hardware Equipment and Software

Exhibit B – Consideration

Exhibit C – Installation Requirements

Exhibit D – Service Level Agreement

2. Provision of License and Services.

2.1. Subject to the terms of this Agreement and the payment of the System Consideration in full, the System Provider shall provide the End-User a limited, exclusive, non-transferable, non-pledgeable and non-assignable license to use the System solely for the End-User's internal use, and for the purpose that it is intended for (the "**License**").

2.2. Subject to provisions of Sections 2.3 and 5.2 below, within one-hundred (100) Business Days following the occurrence of the later of (i) receipt by the System Provider of the Approval, (ii) the completion of the Due-Diligence Process, and (iii) the receipt by the Company of the First Installment, in full, the System Provider shall complete the Deployment and shall conduct the Training.

2.3. The provision of the System, the License and the Services by the System Provider in accordance with the time schedule set forth in Section 2.2 above and the performance by the Company of all its obligations under this Agreement is conditioned upon (i) the fulfillment by the End-User of all of the End-User Responsibilities when due, and (ii) the actual receipt by the Company of each payment of the System Consideration when due, in full.

It is hereby clarified that the Company shall not be held responsible or liable for any delay in the provision of the System, the License and/or the Services, if such delay was due to any miss-performance or delay in the fulfillment of any of the End-User Responsibilities and/or payment obligations and/or due to a delay in the performance or achievement of the pre-requisite conditions set forth in Section 5 below. In the event of a delay in the performance of any of the End-User Responsibilities and/or payment obligations and/or the performance or achievement of the pre requisite conditions set

B 1-2-3

82

forth in Section 5 below, the Company's obligations shall be postponed by such number of days equal to number of days by which the time schedule was delayed due to acts or omissions caused by the End-User.

2.4. If any sum payable pursuant to this Agreement shall not have been paid to the Company by its due date, then, without prejudice to any other right or remedy available to the Company in accordance with the terms of this Agreement or by law, the End-User shall pay interest thereon at a daily rate of 0.04%, accumulated on a daily basis, in respect of the period starting on the due date of the delayed payment and ending on the date of the actual payment. In addition, the Company reserves the right to suspend contractual performance or the use of the System or the Services until the End-User has made payment of the overdue amount together with interest that has accrued thereupon, in full.

2.5. So long as the System Consideration is not received by the Company, in full, and so long as the Company has not provided the Commissioning Notice, the End-User shall not be entitled to use the System and no license to use the System shall be deemed granted.

3. Consideration; Payment Terms.

3.1. In consideration for the provision of the License, the System and the Services, the End-User shall pay the Company the System Consideration as set forth in Exhibit B.

3.2. The System Consideration shall be paid by the End-User to the Company in installments as set forth in Exhibit B.

3.3. The System Consideration, the Support Period Consideration and any other payments made to the Company under this Agreement are exclusive of all state, provincial, municipal or other government, excise, use, sales, VAT or like taxes, tariffs, duties or surcharges, now in force or as may be enacted in the future, which shall be borne by the Company, provided, however that the Company shall bear all income taxes imposed on the Company in connection with this Agreement. Each payment under this Agreement shall be paid by the End-User against an invoice to be issued by the Company.

3.4. Any and all amounts paid to the Company under this Agreement are non-refundable, and may not be claimed or reclaimed by the End-User.

4. The End-User's Responsibilities. The End-User undertakes to perform all of the following obligations in a timely manner (the "**End-User Responsibilities**"):

4.1. fulfillment of all of the technical and installation requirements listed in Exhibit C at the End-User's site, prior to the delivery of the Hardware Equipment;

4.2. obtainment and maintenance of all permits and approvals required to be obtained from any regulatory and governmental authority relating to the End-User, under any and all applicable legal requirements for the performance of this Agreement;

4.3. delivery of the Certificate to the Company;

4.4. provision of any and all applicable information and documents required by the System Provider for the performance of the Due-Diligence Process, on a timely manner; and

4.5. provision of any and all additional required conditions to enable the performance of the Company's obligations under this Agreement when due, including without limitation, release of the Hardware Equipment from custom (if required) and assuring availability of the End-User's personnel for participation in the Training.

5. Pre-Conditions.

5.1. The provision of the License, the System and the Services and the performance by the Company of its obligations under this Agreement are subject to (i) the receipt by the System Provider of the original certificate indicating the identity of the End-User, in accordance with the requirements of the IMOD (the "**Certificate**"), (ii) the receipt by the System Provider of the approval of the IMOD for the provision of the License, System and the Services as set forth herein (the "**Approval**"), (iii) the completion of a due-diligence process to the Company by the System Provider (the "**Due-Diligence Process**").

5.2. For the avoidance of any doubt, no products, licenses, equipment or services shall be provided by the Company under this Agreement until the Certificate is delivered to the System Provider and the Approval is obtained. In the event that the Certificate is not received by the System Provider and/or the Approval is not obtained within six (6) months as of the date hereof, or in the event that the System Provider receives, earlier, a formal notice from the IMOD that the application for the Approval is denied, or in the event that the Approval is canceled, terminated or suspended, the Company shall have the right to terminate this Agreement by providing the End-User a written notice, and such termination shall not be considered a breach of this Agreement, and the Company shall not be held responsible or liable in connection with such termination. Further, the Company hereby acknowledges and agrees that the actual performance of the activities contemplated herein is conditioned upon the completion of the Due Diligence Process to the System Provider's full satisfaction which otherwise may terminate this Agreement at its sole discretion, by providing the Company a written notice, and such termination shall not be considered a breach of this Agreement, and the Company. shall not be held responsible or liable in connection with such termination.

6. Technical Support and Maintenance Services. Following the expiration of the Warranty Period, the End-User shall be entitled to purchase technical support and maintenance services (the "**Support Services**") under the following terms:

6.1. The End-User may purchase Support Services for periods of twelve (12) month each (each such period – a "**Support Period**").

6.2. The Support Services shall be provided in accordance with the System Provider's standard services level agreement, as may be amended from time to time. A copy of the System Provider's current service level agreement is attached hereto as Exhibit D (the "**SLA**").

6.3. The consideration for the Support Services for each Support Period and the payment terms of such consideration are as set forth in Exhibit B.

7. Additional Remedy. In the event a breach has occurred, in addition to the Company's rights and remedies under applicable law and this Agreement, the Company may suspend or cancel the License or the provision of any of the Services, or take such actions necessary to prevent access to the System until such time as it has received confirmation to its satisfaction that such breach was cured. The Company shall not be liable towards the End-User for any claim, losses or damages whatsoever related to its decision to suspend or cancel the provision of any of the Services, the License, or to prevent access to the System under this section.

8. Intellectual Property Rights. All the rights pertaining to the System, the Services and the License, including, but not limited to, all patents, trademarks, copyrights, service marks, trade names, technology, know how, moral rights and trade secrets, all applications for any of the foregoing, and all permits, grants and licenses or other rights relating to the System and the Services are and shall remain the sole property of the System Provider.

The End-User hereby acknowledges that, other than as set forth in Section 2.1, no title to the System (including the software embedded therein) is transferred to it under this Agreement or in connection hereof and it is not granted any right in the System, including without limitation, intellectual property right.

The End-User shall not, whether directly or indirectly either by themselves or through any other person, reproduce, modify, disassemble or reverse-engineer the System (including any software contained therein).

9. Confidentiality. The End-User undertakes to keep the Confidential Information in strict confidence and not to disclose it to any third party without the prior written consent of the

System Provider; provided, however, that the End-User may disclose such information to its respective employees and consultants having a need to know such information in order to carry out the provisions of this Agreement. The End-User warrants that any such employees and consultants to which Confidential Information is disclosed will be bound and will abide by terms no less onerous than those contained herein and shall be responsible for any breach of confidentiality by such employees and consultants.

Following the termination of this Agreement for any reason, or upon the Company's first written demand, the End-User shall return to the Company all Confidential Information, including all records, products and samples received, and any copies thereof, whether in its possession or under its control, and shall erase all electronic records thereof, and shall so certify to the Company in writing

10. Limited Warranty. It should be noted that the System Provider does not warrant that the License, the System and the Services provided hereunder will be uninterrupted, error-free, or completely secure. The System Provider does not make, and hereby disclaims, any and all implied warranties, including implied warranties of merchantability, fitness for a particular purpose and non-infringement. Except as otherwise expressly set forth in this Agreement (including any exhibits), the System Provider does not make and hereby disclaims all express warranties. All products, the System and Services provided pursuant to this Agreement are provided or performed on an "as is", "as available" basis.

11. Limitation of Liability. In no event shall the Company be liable for any consequential, incidental, special, indirect or exemplary damages whatsoever, including lost profits, loss of business, loss of revenues, or any other type of damages, whether arising under tort, contract or law. The Company's aggregate liability under this Agreement shall be limited to the consideration actually received by the Company under this Agreement.

12. Governing Law and Jurisdiction. This Agreement shall be governed, construed and enforced in accordance with the laws of the Republic of Ghana.
Any controversy or claim arising under, out of, or in connection with this Agreement, its validity, its interpretation, its execution or any breach or claimed breach thereof, are hereby submitted to the sole and exclusive jurisdiction of the competent courts in the Republic of Ghana.

13. Assignment. This Agreement and the rights and obligations hereunder are not transferable, pledgeable or assignable, by either party without the prior written consent of the other party. However, the System Provider may assign its rights and obligations to a parent, affiliate or subsidiary company and, in the case of a merger or acquisition, to a successor company upon notice to the Company, and provided that the rights of the Company shall not be derogated pursuant to such assignment.

14. Force Majeure. The System Provider and the Company shall not be liable for any failure to perform its obligations under this Agreement due to any action beyond its control, including without limitation: (i) acts of God, such as fires, floods, electrical storms, unusually severe weather and natural catastrophes; (ii) civil disturbances, such as strikes and riots; (iii) acts of aggression, such as explosions, wars, and terrorism; (iv) acts of government, including, without limitation, the actions of regulatory bodies which significantly inhibits or prohibits the System Provider and the Company from performing its obligations under this Agreement (each, a "**Force Majeure**").
In the event of a Force Majeure, the performance of the Company's obligations shall be suspended during the period of existence of such Force Majeure as well as the period reasonably required thereafter to resume the performance of the obligation.

15. No Third Party Beneficiary. This Agreement shall not confer any rights or remedies upon any person other than the parties to this Agreement and their respective successors and permitted assigns.

16. Complete Agreement. This Agreement and the Exhibits hereto constitute the full and entire understanding and agreement between the parties with regard to the subject matters hereof and

thereof and any other written or oral agreement relating to the subject matter hereof existing between the parties is expressly canceled.

17. Representations. N/A.

18. No Set-Off. Notwithstanding any right available to the End-User under law, the End-User shall not be entitled to set-off any amounts due to the Company under this Agreement.

19. Severability. Should any court of competent jurisdiction declare any term of this Agreement void or unenforceable, such declaration shall have no effect on the remaining terms hereof.

20. Interpretation. The titles and headings of the various sections and paragraphs in this Agreement are intended solely for reference and are not intended for any other purpose whatsoever or to explain, modify, or place any construction on any of the provisions of this Agreement.

21. No Waiver. The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.

22. Notices. All notices and demands hereunder shall be in writing and shall be served by personal service or by mail at the address of the receiving party set forth in this Agreement (or at such different address as may be designated by such party by written notice to the other party). All notices or demands by mail shall be certified or registered mail, return receipt requested, by nationally-recognized private express courier, or sent by electronic transmission, with confirmation received, to the telecopy numbered specified below, and shall be deemed complete upon receipt.

In Witness Whereof, the parties hereto have executed this Agreement the day and year first above written.

17-12-2015

Infraloks Development Limited

By:

Mr. George Derek Oppong

Position: Director, Business Development

17-12-2015

National Communication Agency

By:

Mr. William Tevie

Position: Director General

WT

Exhibit A

Description of the System and Services

The System:

The System Provider's Pegasus system is comprised of the following (the "**System**"):

(a) the features and capabilities detailed in the table attached hereto as Exhibit A-1, operational with respect to the Republic of Ghana mobile numbers (residing in the Republic of Ghana), using the System Provider's supported devices running the System Provider's certified versions of Blackberry, Android and iOS operating systems, including **25** concurrent targets; and

(b) the hardware equipment (the "**Hardware Equipment**") and software which are required for the installation of the System, including **5** control stations, as listed in Exhibit A-2 attached hereto.

The Services:

The services related to the System include the following (the "**Services**"):

(a) Deployment of the System at the End-User's site for use with respect to the Republic of Ghana mobile numbers residing in the Republic of Ghana (as set forth in Section (a) above) (the "**Deployment**");

(b) **Two (2)** week training course and one (1) week on-site handover, which shall be held in English (the "**Training**");

(c) 12 months warranty (the "**Warranty Period**") commencing at the date of the provision of the Commissioning Notice, which shall be provided in accordance with the Company's SLA.

No warranty is provided by the System Provider with respect to the hardware components of the System. To the extent permissible, Hardware Equipment warranty will be provided by the System Provider back to back with the warranty provided by the suppliers of the Hardware Equipment.

Exhibit A-1

Features and Capabilities

Supported OS:

Operating System	Versions	Supported Browsers for Installation
iOS	7.x – 9.1	Safari • Clicking on a link will always result in Safari browser
Android	4.x – 5	• Native browser (Webkit based) • Chrome versions 18 up to 45 (excl. 18.0.1025.166) • Focus mainly on Samsung Galaxy devices
BlackBerry	5.x - 7.1	Native browser (Webkit based)

Installation:

	Feature	Description	Comments	Supported in		
				BlackBerry	Android	iOS
Remote Installation	**Push Message**	Infection is done by silently pushing an installation to the device. This method does not require the target engagement.	• Works on most BlackBerry devices • Works on a variety of Android devices (OS 4.x). Depends on the local ROM settings	V	V	
	Crafted Message (SMS, Email and other 3rd party applications)	An innocent message is sent to the target device which contains text and link. The message content and link lure the target to click (only once) and browse to an innocent website. Clicking the link triggers a silent installation which runs in the background.		V	V	V
Infection Assisting Tools	**MMS Fingerprint**	Reveal the target device and OS version by sending an MMS to the device. No user interaction, engagement or message opening is required to receive the device fingerprint.	This feature may be blocked by the local mobile network operator. Feature implementation subjects to site survey results. Note: MMS content appears on the target device.	V	V	V
	Sender ID Spoofing	Set an alphanumeric sender identification for SMS and MMS.	This feature may be blocked by the local mobile network operator. Feature implementation subjects to site survey results.	V	V	V
	Control link URL	Set any DNS to be used as the installation link	Domains to be defined and purchased by the customer	V	V	V

5131

89

	Feature	Description	Comments	Supported in		
				BlackBerry	Android	iOS
Agent Survivability	**Persistency**	The installed collection tool survives device reboot.	Device reboot refers to: • Device restart • Device turn off • Device battery drain	V	V	V
	Factory Reset	The agent collection tool endures device factory reset.	Factory reset, also known as master reset, restores the device original manufacturer settings resulting in permanent erasing all of the information stored on the device.		V	
	Blocking OS Upgrade	The agent collection tool blocks the user from upgrading the OS version.	The device acts like it has the latest OS version or is not allowed to perform off-the-air OS upgrade. Note: Physical OS upgrade is still available.	V	V	V
Agent Uninstall	**Uninstall**	Permanently remove the agent collection tool	Done remotely without any user interaction	V	V	V

B152

90

Collection:

	Feature[1]	Description	Comments	Supported in		
				BlackBerry	Android	iOS
Historical Data Extraction: Extract all existing data from the device. Gain access to historical data.	**Contact details**	Extracts all contacts available on the device including their assigned photos	Extraction is done for all available (non-empty) fields.	V	V	V
	SMS	Extracts all incoming and outgoing text messages (SMS) from the device		V	V	V
	iMessage	Extracts all incoming and outgoing iMessages from the device	Messages sent only between iOS devices			V
	Emails	Extracts all emails that exist on the device	Extracts only from the device stock application and Gmail application. Emails are presented in HTML format.	V	V	V
	Call Log	Extracts the history of all incoming/outgoing calls made to/from the device		V	V	V
	WhatsApp Call Log	Extracts the history of all incoming/outgoing calls made to/from the device using WhatsApp			V	
	Skype Call Log	Extracts the history of all incoming/outgoing calls made to/from the device using Skype			V	V

[1] Due to some limitations and restrictions of the operating system, certain devices might not support all listed features.

5133

91

	Feature[1]	Description	Comments	Supported in		
				BlackBerry	Android	iOS
	Calendar	Extracts all calendar records that exist on the device		V	V	V
	Browsing History	Extract the entire list of browsed websites that exists on the device	Extracts only from the device native browser application		V	V
	BBM (BlackBerry messenger)	Extracts all existing incoming and outgoing instant messages from the device, including personal and group chat	Extracts only instant messages (text)	V		
	WhatsApp			V	V	V
	Viber				V	V
	Skype				V	V
	Facebook Messenger				V	V
	Kakao Talk			V	V	V
	Telegram					V
	Line			V	V	V
	Odnoklassniki				V	V
	WeChat			V	V	V
	Tango				V	V
	VKontakte				V	V
	Mail.Ru				V	V
Data Monitoring: Real-time monitor of new data that arrives/sent to/from the	Contact details	Monitors addition, deletion and editing of contacts on the device		V	V	V
	SMS	Monitors incoming and outgoing text messages		V	V	V
	iMessage	Monitors incoming and outgoing iMessages	Messages sent only between iOS devices			V

B134

92

	Feature	Description	Comments	Supported in		
				BlackBerry	Android	iOS
device	**Emails**	Monitors incoming and outgoing emails	Monitors only the device stock application and Gmail application. Emails are presented in HTML format.	V	V	V
	Call Log	Monitors incoming and outgoing call records		V	V	V
	WhatsApp Call Log	Monitors incoming and outgoing call records of WhatsApp application			V	
	Skype Call Log	Monitors incoming and outgoing call records of Skype application			V	V
	Calendar	Monitors addition and editing of calendar records on the device		V	V	V
	Browsing History	Monitors new browsed websites	Monitors only the device native browser application		V	V
	BBM (BlackBerry Messenger)	Monitors incoming and outgoing instant messages, including personal and group chat	Monitors only instant messages (text). Indication for file transfer appear and their retrieval is possible using file retrieval feature.	V		
	WhatsApp			V	V	V
	Viber				V	V
	Skype				V	V
	Facebook Messenger				V	V
	Kakao Talk			V	V	V
	Telegram					V
	Line			V	V	V
	Odnoklassniki				V	V
	WeChat			V	V	V

B135

93

	Feature	Description	Comments	Supported in		
				BlackBerry	Android	iOS
	Tango				V	V
	VKontakte				V	V
	Mail.Ru				V	V
	surespot				V	V
	USSD	Monitors incoming network messages from the device		V	V	V
	Call recording (call interception)	Record incoming and outgoing voice calls made to/from the device	Calls are recorded locally on the device and then sent to the system servers.	V	V	V
	Device Information	Monitors general details about the device, network and connection		V	V	V
	Cell-ID Location	Monitors the device cell-ID within every connection to the command and control servers		V	V	V
	Keystroke logging	Monitors keystroke typing by the regular keyboard	Helps monitoring texting in unsupported applications and even usernames and passwords for sensitive accounts.		V	
Active Data Collection: User request's real-time actions on target device	Front Camera Snapshot	Take a snapshot using the device front camera	No indication appears on the device and flash is never used.		V	V
	Back Camera Snapshot	Take a snapshot using the device rear camera	No indication appears on the device and flash is never used.	V	V	V
	Screenshot capturing	Capture a screenshot of the device		V	V	V
	File System listing	Retrieve a full list of files and		V	V	V

	Feature	Description	Comments	Supported in		
				BlackBerry	Android	iOS
		folder in target device				
	File retrieval	Retrieve any file from the target device including photos, documents, audio and video	File retrieval is allowed from the device internal storage and SD card.	V	V	V
	GPS Location	Locate device using the device GPS chip		V	V	V
	Room Tap (environmental sound recording)	Turn on the microphone and listen in real-time to the surrounding sounds of the device. The surrounding sounds are recorded and saved for later playback and analysis.	Turning on the microphone is done by issuing an incoming silent call to the device. No indication of the recording or the 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.	V	V	V

7.5.17

95

Data Transmission:

	Feature	Description	Comments	Supported in		
				BlackBerry	Android	iOS
Data Transmission: Channels used to exfiltrate the collected data back to the command and control servers	**GPRS/UTMS/LTE**	Transmit collected data using cellular data channels	Data is sent in very small packets. This has very small impact on target's data plan.	V	V	V
	Wi-Fi	Transmit collected data using Wi-Fi	Has no impact on target's data plan at all.	V	V	V

K1328

96

Presentation:

Feature	Collected Data	Displayed As
Contact details	Entire values stored in the contact entry including photo if available	• Grid • Contact card with the entire details
SMS	• Type (SMS / USSD) • Direction (incoming, outgoing) • Contact name • Phone number • Message content • Date & Time	• Grid
USSD		
iMessage		
Emails	• From • To • CC • Subject • Folder • Account • Message content • Date & Time	• Grid • Full HTML presentation (emulates popular email clients)
Call Log (Cellular calls, WhatsApp, Skype)	• Direction • Contact name • Phone number • Duration • Date & Time	• Grid
Calendar	• Meeting subject • Location • Event date and start time	• Grid • Monthly calendar view (emulates popular calendar clients)

1527

47

Feature	Collected Data	Displayed As
Browsing History	• Website name (as saved by the target, usually the default website name) • Website URL address	• List
BBM (BlackBerry Messenger)	• Type of application • Chat participants (Names & phones) • Conversation content • Date & Time • Attachments metadata (without the attachment)	• Grid • Conversation mode
WhatsApp		
Viber		
Skype		
Facebook Messenger		
Kakao Talk		
Telegram		
Line		
Odnoklassniki		
WeChat		
Tango		
VKontakte		
Mail.Ru		
surespot		
Call recording (call interception)	• Direction • Contact name • Phone number • Duration • Date & Time	• Grid • Playback interface

15140

78

Feature	Collected Data	Displayed As
Device and Network Information	• Battery level • Last location • Connection type (e.g., 3G, WiFi) • MSISDN • IMEI • IMSI • Device Manufacturer • Device model • Operating System version • Installation type (remote, physical or other) • Installation date • Last communication time • Next communication expected • Device current country • Device home country • Serving network • Home serving network	• Dashboard
GPS/Cell-ID Location	• Data source (GPS/Cell-ID) • Latitude • Longitude • Enter Time & Date • Leave Time & Date	• Grid • Map: - On map display - Full trail - Type of location data (GPS or Cell-ID based)
Keystroke logging	Text typed using the keyboard	• List
Front Camera Snapshot	• Date & Time • Photo • Source of photo	• Grid • Photo viewer
Back Camera Snapshot		
Screenshot capturing		

Feature	Collected Data	Displayed As
File System listing	• List of folders (tree) • List of files (grid): - Filename - Modified date - File size - Retrieval status	• Grid • Tree view
File retrieval		
Room Tap (environmental sound recording)	• Recorded audio • Recording Date & Time • Duration	• Grid • Playback interface

B141

100

Rules & Alerts:

Rule Type	Alert When	Alert Description
Geo Fence - Access hotspot	Alert when target entered an important area	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	The alert occurs in two target are at the same perimeter as defined by the user. The alert will take place also if targets visited the same location in different times.
Connection detection	Alert when a message is sent from/to a specific number	Alert when target is corresponding with a certain number as defined by the user.
	Alert when a phone call is performed from/to a specific number	Alert when target conducts/receives a phone call to/from a certain number as defined by the user.

8142

101

Exhibit A-2

List of Hardware Equipment and Software

The System Provider shall supply the following hardware equipment and software, or similar, to enable the commissioning of the system.

Disclaimer: This list may change per Network\Regulation\System\Country feature support changes.

Item Description	Manufacturer	QTY	Device Model
PowerEdge R730xd Server Intel Xeon E5-2643 v3 3.4GHz,20M Cache,9.60GT/s QPI,Turbo,HT,6C/12T (135W) Max Mem 2133MHz R730/xd PCIe Riser 2, Center R730/xd PCIe Riser 1, Right PowerEdge R730xd Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) Bezel Chassis with up to 24, 2.5" Hard Drives DIMM Blanks for System with 2 Processors Performance Optimized 2133MT/s RDIMMs 8 X 8GB RDIMM, 2133MT/s, Dual Rank, x8 Data Width 2 X Standard Heatsink for PowerEdge R730/R730xd Upgrade to Two Intel Xeon E5-2643 v3 3.4GHz,20M Cache,9.60GT/s QPI,Turbo,HT,6C/12T (135W) iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise 2 X 300GB 15K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive,13G 16 X 500GB 7.2K RPM NLSAS 6Gbps 2.5in Hot-plug Hard Drive,13G PERC H730 Integrated RAID Controller, 1GB Cache Performance BIOS Settings Dual, Hot-plug, Redundant Power Supply (1+1), 750W 2 X C13 to C14, PDU Style, 10 AMP, 0.6m Power Cord PowerEdge Server FIPS TPM Intel Ethernet i350 QP 1Gb Network Daughter Card Intel Ethernet I350 QP 1Gb Server Adapter	Dell	1	R730XD

B143

102

Item Description	Manufacturer	QTY	Device Model
PowerEdge R730/R730xd Motherboard No Media Required No Operating System OpenManage Essentials, Server Configuration Management Electronic System Documentation and OpenManage DVD Kit, PowerEdge R730/xd OEM Order Not Selected in this Configuration Asset Service - System & Shipbox Label (Model, Svc Tag, Order Information, Basic Config Details) ReadyRails Sliding Rails With Cable Management Arm RAID 1+RAID 5 for H330/H730/H730P (2 + 3-22 HDDs or SSDs) Base Warranty 1Yr Parts Only Warranty (Emerging Only) INFO 1Yr ProSupport and Next Business Day On-Site Service (Emerging Only) 3Yr ProSupport and Next Business Day On-Site Service (Emerging Only) Consolidation Fee EX-Works			
PowerEdge R730 Server Intel Xeon E5-2620 v3 2.4GHz,15M Cache,8.00GT/s QPI,Turbo,HT,6C/12T (85W) Max Mem 1866MHz R730/xd PCIe Riser 2, Center R730 PCIe Riser 3, Left R730/xd PCIe Riser 1, Right PowerEdge R730 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) Bezel Chassis with up to 8, 3.5" Hard Drives DIMM Blanks for System with 2 Processors Performance Optimized 2133MT/s RDIMMs 2 X 8GB RDIMM, 2133MT/s, Dual Rank, x8 Data Width 2 X Standard Heatsink for PowerEdge R730/R730xd Upgrade to Two Intel Xeon E5-2620 v3 2.4GHz,15M Cache,8.00GT/s QPI,Turbo,HT,6C/12T (85W)	Dell	2	R730

Item Description	Manufacturer	QTY	Device Model
iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise 2 X 300GB 10K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive,3.5in HYB CARR PERC H730 Integrated RAID Controller, 1GB Cache Performance BIOS Settings DVD+/-RW, SATA, Internal Dual, Hot-plug, Redundant Power Supply (1+1), 750W C13 to C14, PDU Style, 10 AMP, 0.6m Power Cord European Power Cord 220V PowerEdge Server FIPS TPM Intel Ethernet i350 QP 1Gb Network Daughter Card Intel Ethernet I350 QP 1Gb Server Adapter PowerEdge R730/R730xd Motherboard No Media Required No Operating System OpenManage Essentials, Server Configuration Management Electronic System Documentation and OpenManage DVD Kit, PowerEdge R730/xd OEM Order Not Selected in this Configuration Asset Service - System & Shipbox Label (Model, Svc Tag, Order Information, Basic Config Details) ReadyRails Sliding Rails With Cable Management Arm RAID 1 for H330/H730/H730P (2 HDDs or SSDs) Base Warranty 1Yr Parts Only Warranty (Emerging Only) INFO 1Yr ProSupport and Next Business Day On-Site Service (Emerging Only) 3Yr ProSupport and Next Business Day On-Site Service (Emerging Only) Consolidation Fee EX-Works			
PowerEdge R730 Server Intel Xeon E5-2650 v3 2.3GHz,25M Cache,9.60GT/s QPI,Turbo,HT,10C/20T (105W) Max Mem 2133MHz R730/xd PCIe Riser 2, Center R730 PCIe Riser 3, Left R730/xd PCIe Riser 1, Right	Dell	2	R730

Item Description	Manufacturer	QTY	Device Model
PowerEdge R730 Shipping EMEA1 (English/French/German/Spanish/Russian/Hebrew) Bezel Chassis with up to 8, 3.5" Hard Drives DIMM Blanks for System with 2 Processors Performance Optimized 2133MT/s RDIMMs 8 X 16GB RDIMM, 2133 MT/s, Dual Rank, x4 Data Width 2 X Standard Heatsink for PowerEdge R730/R730xd Upgrade to Two Intel Xeon E5-2650 v3 2.3GHz,25M Cache,9.60GT/s QPI,Turbo,HT,10C/20T (105W) iDRAC8 Enterprise, integrated Dell Remote Access Controller, Enterprise VFlash, 8GB SD Card for iDRAC Enterprise 2 X 300GB 10K RPM SAS 6Gbps 2.5in Hot-plug Hard Drive,3.5in HYB CARR PERC H730 Integrated RAID Controller, 1GB Cache Emulex LPE12002 Dual Channel 8Gb PCIe Host Bus Adapter, Low Profile Performance BIOS Settings DVD+/-RW, SATA, Internal Dual, Hot-plug, Redundant Power Supply (1+1), 750W C13 to C14, PDU Style, 10 AMP, 0.6m Power Cord PowerEdge Server FIPS TPM Intel Ethernet i350 QP 1Gb Network Daughter Card Intel Ethernet I350 QP 1Gb Server Adapter PowerEdge R730/R730xd Motherboard No Media Required No Operating System Electronic System Documentation and OpenManage DVD Kit, PowerEdge R730/xd OEM Order Not Selected in this Configuration Asset Service - System & Shipbox Label (Model, Svc Tag, Order Information, Basic Config Details) ReadyRails Sliding Rails With Cable Management Arm RAID 1 for H330/H730/H730P (2 HDDs or SSDs) Base Warranty 1Yr Parts Only Warranty (Emerging Only)			

5146

105

Item Description	Manufacturer	QTY	Device Model
INFO 1Yr ProSupport and Next Business Day On-Site Service (Emerging Only) 3Yr ProSupport and Next Business Day On-Site Service (Emerging Only) Consolidation Fee EX-Works			
PowerEdge KVM 1081AD - 8 Port Keyboard/Video/Mouse Analog Switch, EUCEM 8x USB Server Interface Pod, includes 2 CAT 5 Cables, TAA	Dell	1	1081AD
1U KMM (Touchpad, US/International Keyboard and Widescreen 18.5" LED) with ReadyRails - Kit	Dell	1	
FAS8020A-001-R6 FAS8020 High Availability System 7-Mode 2 X6226-R6-C Chassis,FAS8020,AC PS,-C 1 X6554-R6-C Cable,Cntlr-Shelf/Switch,15m,LC/LC,Op,-C 4 X6559-R6-C Cable,SAS Cntlr-Shelf/Shelf-Shelf/HA,5m,-C 8 X6562-R6-C Cable,Ethernet,5m RJ45 CAT6,-C 4 X6585-R6-C Cable,Ethernet,3m RJ45 CAT6,-C 1 X2065A-EN-R6-C HBA SAS 4-Port Copper 3/6 Gb QSFP PCIe,EN,-C 2 X5515A-R6-C Rackmount Kit,4N2,DS14-Middle,-C,R6 1 X5526A-R6-C Rackmount Kit,4-Post,Universal,-C,R6 2 X6596-R6-C SFP+ FC Optical 16Gb,-C 4 DOC-8020-C Documents,8020,-C 1 X1973A-R6-C Flash Cache 512GB PCIe Module 2,-C 2 X800-42U-R6-C Power Cable,In-Cabinet,C13-C14,-C 6 DS2246-1014-24S-0P-R6-C DSK SHLF,24x600GB,10K,0P,-C 2 SW-2-8020A-CIFS-C SW-2,CIFS,8020A,-C 2 SW-2-8020A-FCP-C SW-2,FCP,8020A,-C 2 SW-2-8020A-ISCSI-C SW-2,iSCSI,8020A,-C 2 SW-2-8020A-NFS-C SW-2,NFS,8020A,-C 2 OS-ONTAP-CAP2-0P-C OS Enable,Per-0.1TB,ONTAP,Perf-Stor,0P,-C 288	NetApp	1	FAS8020

1547

108

Item Description	Manufacturer	QTY	Device Model
Digi PortServer TS 16 port rackmountable RJ-45 Serial to Ethernet Terminal Server	Digium	2	TS 16
One (1) span digital T1/E1/J1/PRI PCI-Express x1 card	Digium	2	
Cisco 2921 Cisco 2921 Security Bundle w/SEC license PAK SMARTNET 8X5XNBD Cisco 2921 Security Four port 10/100/1000 Ethernet switch interface card Cisco 2901-2921 IOS UNIVERSAL Data Paper PAK for Cisco 2901-2951 Cisco 2921/2951 AC Power Supply Console Cable 6ft with RJ45 and DB9F Cisco Config Pro Express on Router Flash Insert Packout - PI-MSE IP Base License for Cisco 2901-2951 Blank faceplate for HWIC slot on Cisco ISR 512MB DRAM for Cisco 2901-2921 ISR (Default) 256MB Compact Flash for Cisco 1900 2900 3900 ISR Security License for Cisco 2901-2951 Blank faceplate for DW slot on Cisco 2951 and 3925 Removable faceplate for SM slot on Cisco 290039004400 ISR	Cisco	3	2921
Cisco 3750X Catalyst 3750X 48 Port Data IP Base SMARTNET 8X5XNBD Catalyst 3750X 48 Port Data IP Base for 36 Months Catalyst 3K-X 350W AC Secondary Power Supply CAT 3750X IOS UNIVERSAL WITH WEB BASE DEV MGR Cisco StackWise 50CM Stacking Cable Catalyst 3750X and 3850 Stack Power Cable 30 CM Catalyst 3K-X 10G Network Module Catalyst 3K-X 350W AC Power Supply Insert Packout - PI-MSE	Cisco	2	Cisco 3750X

8/4/15

107

Item Description	Manufacturer	QTY	Device Model
Catalyst 2960-X 48 GigE 4 x SFP LAN Base SMARTNET 8X5XNBD Cat 2960-X Stk 24 GigE4xSFP LAN Base (36 Months) Insert Packout - PI-MSE	Cisco	2	Cisco 2960-X
Cinterion MC55i Modem	Cinterion	9	MC55i
Optiplex 7010 MT · OptiPlex 7010 MT : Mini-Tower · Windows 8 · 3rd Gen Intel Core i7-3770 (Quad Core, 3.40GHz Turbo, 8MB, w/ HD4000 Graphics · 8GB (2X4GB) 1600 MHz DDR3 Non-ECC · UK/Irish (QWERTY) Dell KB212-B QuietKey USB Keyboard Black · 1TB 3.5inch Serial ATA III (7.200 Rpm) Hard Drive · Dell Optical (Not Wireless), Scroll USB (3 buttons scroll) Black Mouse · 16XDVD+/-RW Drive · Internal Dell Business Audio Speaker · 3Yr ProSupport and Next Business Day On-Site Service (Emerging Only)	Dell	15	
Dell Professional P2314H 58.4cm(23") LED monitor VGA,DVI-D,DP (1920x1080) Black UK	Dell	30	
APC NetShelter SX 42U Deep Enclosure 1200X600 with Roof and Sides Black	APC	2	AR3300
Rack PDU 2G, Metered, ZeroU, 32A, 230V, (36) C13 & (6) C19	APC	4	AP8853
PDU Cord Retention Kit for Full-Height & 48U, Basic & LCD-Metered PDU (1 per PDU	APC	4	AP9569
Horizontal Cable Organizer 1U w/brush strip		10	AR8429
Cat7 patch cord,0.5m,BLue		20	
Cat7 patch cord,1m,BLue		40	

Item Description	Manufacturer	QTY	Device Model
Cat7 patch cord,2m,BLue		60	
Cat 7 patch cord,5m,BLACK		20	
Cat 7 patch cord,10m,Grey		10	
48 port Cat 6 patch Panel HD Netkey		4	
duplex patch cord,10m - Patch cord Fiber OM3 LC LC 10m		10	
Console Cable 6ft with RJ45 and DB9F		2	
Blank plate 1U(10 per pack total 4 packs)		40	
Power Cord, C13 to C14, 5m		20	
Power Cord, C13 to C14, 3m		40	
APC Smart-UPS SRT 5000VA RM 230V	APC	4	SRT5KRMXLI
APC Smart-UPS SRT 5kVA Output HW Kit	APC	4	SRT001
SRT001 Kit installation	APC	4	
power cable 3 meters for ups + Sicon 32A	APC	4	
APC Smart-UPS SRT 192V 5kVA and 6kVA RM Battery Pack	APC	4	SRT192RMBP
Office Pro Plus 2013	Microsoft	15	
VPP L3 VMware vSphere 5 Enterprise for 1 processor Production Support/Subscription for VMware vSphere 5 Enterprise for 1 processor	Vmware	4 processors	
VPP L3 VMware vCenter Server 5 Standard for vSphere 5 (Per Instance)	Vmware	1 Instances	

B150

109

Item Description	Manufacturer	QTY	Device Model
Veeam Backup & Replication Enterprise for Vmware and Hyper-V per Socket License	Veeam	6 Sockets	
Microsoft Windows Server 2012 R2 Standard Edition 2 Socket License	Microsoft	2	
MS SQL 2014 Server Standard core 2 socket License	Microsoft	2	
Nagios XI (Enterprise version with 100 Nodes license)	Nagios	1	

B152

97

Exhibit B

Considerations

Considerations Amounts

Definition	Consideration for	Amount in USD
"System Consideration"	provision of the License, System and Services.	8,000,000 (eight million)
"Support Period Consideration"	any one Support Period.	22 % of the System Consideration.

Payment Terms

System Consideration

The System Consideration shall be paid by the End-User to the Company in three (3) installments as follows:

(a) 50% of the System Consideration shall be paid by January 28th, 2016 (the "**First Installment**").

(b) 35% of the System Consideration shall be paid upon the provision of the Hardware Equipment to the End-User's site.

(c) 15% of the System Consideration shall be paid upon the provision of a written notice by the Company to the End-User confirming that the Deployment of the System at the End-User's site was completed (the "**Commissioning Notice**").

Support Period Consideration

The Support Period Consideration shall be paid in one payment, in advance of each Support Period.

Exhibit C

Installation Requirements

The End-User shall ensure that the following pre-requisites are ready 2 weeks prior to the System installation (aligned to SW version).

Disclaimer: This list may change per Network\Regulation\System feature support changes.

Prerequisite	Equipment	Remarks
Internet Connection	2 symmetric ATM lines each 20MB (from 2 different ISP's) with static IP's of 8 external addresses	2 lines are required for redundancy. The minimum requirement might be even lower - depends on the number and type of end stations.
Cellular Reception	Stable Cellular Reception	~-95 db
Air Condition	18 Degrees	None
Electricity	4 power socket - 220V	Server room and operational room drawings are required to accurately specify all wall outlets location. Power generator and Facility environment against hazard dangers are optional
Area needed for server room	5X5M, Height 2.5 M	There are 2 48U racks with the following dimensions: Height 2258.00 mm, Width 600.00 mm, Depth 1070.00 mm
Area needed for operator room	10X10M, Height 2.5 M	Can be divided into separate rooms
Patch panel	Depends on the number of stationary stations. Wires from the end stations to the patch panel in the rack	
SIMs	2 SIM cards for each network	It is mandatory to use a 3rd party to order the SIMs , also use a postpaid account
Security	Lockable doors	
Untraceable payment method	1 X named credit card with 4000$ balance 1 X Passport scan on the same name as a credit card 1 X Prepaid no name local SIM card 1 X Utility bill with address on the same name as Passport	It is recommended to use a 3rd party, The passport, credit card and utility bill should not be related to the organization

Exhibit D

Service Level Agreement

1. Introduction

This Service Level Agreement (the "**SLA**") is an agreement between NSO Group Technologies Ltd. (hereinafter the "**Company**") and Infralok Development Limited (hereinafter the "**Reseller**").

The purpose of this SLA is to specify the services and commitments with respect to the software technical support, location support and/or hardware replacement services for the purchased products.

1.1. Objectives of the Service Level Agreement

To create an environment which is conducive to a co-operative and productive relationship between the Company, the End User, and the Reseller to ensure effective support for the End User.

To document the responsibilities of all the parties involved in the SLA.

To ensure the Company provides high quality service to the Reseller and the End User.

To define the service to be delivered by the Company and the level of service which can be expected by the End User, thereby reducing the risk of misunderstandings.

To institute a formal system of objective service level monitoring ensuring that reviews of the SLA are based on factual data.

To provide a common understanding of service requirements/capabilities and of the principals involved in the measurement of service levels.

To provide for all parties to this SLA a single, easily referenced document, which caters for all objectives as listed above.

GD

B155 114

14

2. Definitions

Hardware Replacement means a HW replacement service for the hardware products purchased by the Reseller from the Company, whereby the Company delivers a replacement to the End User's site before the End User returns the faulty hardware.

All Hardware Replacements shall take effect after the Company receives relevant alerts and all required information, and determines that the hardware issue is related to a malfunction of one of the hardware components.

Business Day means a normal working day in the time zone where the End User is located.

Device Number means a unique identifier of a hardware device, which can be located on a label on a Hardware product:

- Media Access Control (**MAC**) Address,
- Serial Number (**S/N**),
- Service Tag Number (**STN**)
- International Mobile Station Equipment Identity (**IMEI**)

Documentation means the User and Technical manuals provided by the Company for use with the purchased software and hardware products.

Enhancement means all software changes, including new releases, new versions, product improvements, system modifications, updates, upgrades and service packs.

Error means an error in one or more of the Company's products, which degrades the product functionality in accordance with the Severity definitions, as compared to the product functionality and performance specifications described in the official user guides provided by the Company.

Hardware means a computing device and/or its component with a specific function and limited configuration ability. The Hardware is sold by the Company to the Reseller for the sole purpose of executing the specific Software product/s supplied with it.

Information means any idea, data and program, technical, business or other intangible information, however conveyed.

Problem Resolution means the use of reasonable commercial efforts to resolve the reported problem. These methods may include, but are not limited to: configuration changes, patches that fix an issue, replacing a failed hardware component, reinstalling the software, etc.

Force Majeure has the meaning ascribed to it in the Agreement between the parties.

Response means addressing the initial request and commencement of work pertaining to the issue.

Response Time means the amount of time elapsed between the initial contact by the Reseller or the End User with the Company's Technical Support Team and the returned response to the Reseller or the End User by the Company's support staff.

Resolution Time means the amount of time elapsed between the initial contact by the Reseller or the End User with the Company's Technical Support Team till the issue reported is resolved wither by permanent fix or a workaround till a permanent fix would be available.

Security Code means a specific code dedicated to the End User's account in the Company's Technical Support Center. This code must be provided by the End User each time the End User approaches the Company's support staff.

Support means the technical Support and Hardware replacement services provided by the Company to the End User as set forth in this SLA.

Support case means a single issue opened in the Company's Case Management System. The case number identifies the Service Request.

Field Service Engineer means an engineer that provides the following onsite services: installation, field configuration, operates system to demonstrate equipment on test devices and to analyze malfunctions, interprets maintenance manuals, schematics, and diagrams, and repairs electronic equipment, such as computer, computing device or component, utilizing knowledge of electronics and using standard test instruments and hand tools.

System means the Hardware, Software and Documentation that have been provided to the Reseller and/or the End User by the Company.

Workaround means a change in the followed procedures or data to avoid error without substantially impairing use of the product.

GUD

WT

16 15 7 116

3. Company's Obligations

3.1. Maintenance and Support

The Services shall include warranty, support and maintenance of the System as further detailed below, via support center.

The Company shall provide the End User with technical support for the System, consisting of: (a) first level to fourth level ("**Tier1 to Tier4**" as described in section 6.2) support via the Company's support center, and (b) SW updates and SW upgrades of the System, which, for the avoidance of any doubt, shall not be specifically adjusted to comply with any End-User Adjustments (as such term is defined in the Agreement which this SLA is attached to). The Services shall only be provided to the End User

System support and maintenance covers both SW and HW provided by the company. In case of 3rd party HW supplier, the company will contact the 3rd party and ensure proper support provided to the End User.

Maintenance will cover the following:

a. **SW upgrades** – periodical SW releases to add new features and bug fixes. Installing a new SW upgrade is communicated in advance to schedule the best time for the end-user and minimize the system downtime

b. **SW updates** – special SW packages provided to fix specific critical bug outside the periodical SW release. SW updates are also provided when a new OS version is introduced for a specific platform (e.g new iOS version).

c. **Monitoring system** – connected to our 24/7 NOC room and monitored around the clock. The monitoring system is configured to do the following:

    a. Connected to all the major HW components in the system, providing real-time status of the system.

    b. Monitors SW components such as tunnels, VPS servers alerting when any component goes down

    c. Checks for white accounts balances and alerts when it is below a predefined threshold

    For further details, see the enclosed "System monitoring capabilities and requirements" appendix.

d. **24/7 support** – A dedicated NOC center is operated to provide 24/7 support. Tickets can be submitted via phone call, dedicated website or email. The NOC representatives follow our support procedures to ensure each ticket is being handled according to the SLA.

End user should report issues with the system, using an agreed form or tool specifying all predefined data and providing all the required operational and technical information

The Company shall not be obligated to provide the Services in case of misuse, abuse, neglect, alteration, modification, improper installation of the System, use of the System for purposes other than those authorized by the Company, or repairs by anyone other than the Company or its authorized representatives without the Company prior written approval. The Company shall not be obligated to provide the Services in connection with the End-User Adjustments.

3.2. Software Support

For End Users covered under a valid Support offering, Software Support will be provided pursuant to the terms of **Section 6 "Software Support Procedure"**. The scope of commitment in case of System failure requiring a software repair or fix is to preserve the System at the fully functional condition as per the acceptance data of the System by the End User.

Software fixes are generally delivered in a secure format, delivered by the Company or in special occasions by the Reseller and/or the End User or third party partner if it is agreed for a particular case. In addition, permanent fixes are developed for known non-critical issues. These are incorporated into service pack updates that are periodically distributed. The version updates may include additional features, bug fixes and/ or services.

The Company agrees to provide Support, where appropriate to the End User, which may include but is not limited to, the following actions:

(a) Provide the End User with access to product update releases and related Documentation, upon general commercial release.

(b) Provide the End User with access to Technical Support Team representatives, who will work with the End User to diagnose issues, and provide Problem Resolutions, including escalating the issue as needed.

3.3. Hardware Replacement

For End Users covered under a valid Support offering, the Company will use commercially reasonable efforts to provide Hardware replacement in accordance with the terms set forth in **Section 5 "Hardware Replacement Procedure"**. Provision of hardware Replacement is subject to the following limitations:

(a) The Company will provide Hardware Replacement for up to three (3) years after hardware installation at the End User's Site or according to standard Hardware in case of a 3rd party supplier.

(b) Hardware shall be repaired or replaced with same or similar products when needed, at the Company's discretion.

3.4. On-site Hardware Support

For End Users covered under a valid Support offering, upon the End User's request, after the Company determines that the hardware issue is related to a malfunction of one of the hardware components, the Company will decide whether to dispatch a representative to the site.

Provision of on-site support is subject to the following limitations:

(a) On-site Hardware Support does not include on-site service for Software troubleshooting or any Software or training related issues.

(b) On-site Hardware Support service may not dispatch a representative on-site to perform Hardware replacement outside of the End User's Site address for the Hardware.

(c) On-site service response times may be dependent upon the End User's Site address for the Hardware, the timely arrival of replacement parts at the End User's Site, and accessibility to the Site.

3.5. On-site Software Support

On-site Software Support applies only in cases of Severity 1 issues which can't be solved remotely (based on the Company's customer support staff judgment). After the Company confirms that the matter is a Severity 1 issue, the Company and the End User will work diligently, with highly skilled engineers to resolve the critical situation and to restore operation.

In case the criticality of the issue remains or no progress is made, the Company will decide whether to dispatch a representative to the End User's Site or use a partner Support representative.

3.6. Exclusions

Support does not include the following items or actions:

(a) Step-by-step installation of Software or Service Packs.

(b) On-site services (outside the ones described in this SLA), Professional Services, Managed Services, or Educational Services.

(c) Modification of software code, IT Network architecture changes, Security-policy configuration, Audits, or Security design.

The Company shall have no obligation to Support:

(a) An altered, damaged, or modified product or any portion of the product incorporated with or into other software, hardware, or products not specifically approved in advance in writing by the Company.

(b) Product problems caused by the Reseller's and/or the End User's negligence, misuse, misapplication, or use of the product in a way other than as specified in the System user manual, or any other causes beyond the control of the Company.

(c) Product installed on any computer hardware that is not supported by the Company.

(d) Product not purchased from the Company.

(e) Products subjected to unusual physical or electrical stress, misuse, negligence or accident, or used in ultra-hazardous activities.

The Company shall have no obligation to Support the End User if:

(a) Appropriate payment for Support has not been received by the Company and the Reseller and/or the End User is unable to show reasonable proof of such payment; or

(b) The End User's annual Support term has expired without renewal.

5. Hardware Replacement Procedure

The Company uses equipment from leading vendors, surveillance, network servers and software remedies. With each manufacturer, the Company has a contract for Service and Customer technical support.

For End Users covered under a valid Support offering, the Company will provide the following Hardware Support:

(a) The Company will attempt to diagnose and resolve Hardware problems over the phone or via remote access. Upon determination that an issue is related to a malfunction of one of the Hardware components, the Hardware Replacement process will be initiated by the Company.

(b) The Company will either issue a replacement for the faulty part or a full Hardware product replacement.

(c) The Company will send the required hardware to the End User's Site location within thirty (30) business days of Hardware Replacement process initiation. The time to ship the required hardware is dependent also on the export procedures that the Company must comply with, as well as the import procedures on the End User's side.

(d) The End User must ship back the faulty Hardware product (or replaceable unit) suitably packaged, as specified by the Company in a letter shipped with the replacement, to a location designated by the Company.

(e) Return shipment of the faulty Hardware should be made within five (5) business days of the arrival of the replacement. Transportation costs for return shipment shall be borne by the End User.

(f) Transportation costs incurred in connection with the delivery of a repaired or replacement item to the End User by the Company shall be borne by the Company; provided, however, that if the Company determines, in its sole discretion, that the allegedly defective item is not covered by the terms and conditions of the Hardware Support described in this SLA or that a claim is made after the Hardware Support period expired, the cost of the repair or replacement by the Company, including all shipping expenses, shall be reimbursed by the End User.

(g) The Company shall have no obligation to Support and Replace Hardware not monitored by Monitoring Client installed on the System and connected to the Company's Technical Support Center.

The Company shall have no obligation to Support:

(a) An altered, damaged, or modified product or any portion of the product incorporated with or into other software, hardware, or products not specifically approved in writing by the Company.

(b) Product problems caused by the End User's negligence, misuse, misapplication, or use of the product other than as specified in the System user manual, or any other causes beyond the control of the Company.

(c) Products subjected to unusual physical or electrical stress, misuse, negligence or accident, or used in ultra-hazardous activities.

(d) Untrained personnel from the End User are operating the system.

6. Software Support Procedure

(a) Upon initiation of initial contact with the Company's Technical Support Center, the End User must authenticate its identity by providing a valid **Security Code**. The Company shall have no obligation to provide Support if the End User does not provide the code.

(b) A Technical Support representative will validate the **Security Code** and start gathering details relevant to the question or issue. The Company shall have no obligation to provide Support services if the End User does not provide the relevant information.

(c) A unique Support Case number **[Trouble Ticket]** will be assigned and delivered to the End User either verbally or via email. This number will be used to track any given issue from initial contact to final Problem Resolution.

(d) If appropriate, an issue will be reproduced in the Company's labs. Additional testing and problem duplication may take place in a network laboratory environment. Further investigation, including additional troubleshooting or debugging activity may be required. Based on the results of the Test Lab investigation, an issue may be resolved, or, if an anomaly is identified, elevated to the appropriate Company's Team for final Problem Resolution.

(e) The Company agrees to use commercially reasonable efforts to work with the End User on Problem Resolution for an issue in accordance with the specifications of this SLA. Timely efforts must be made by all parties involved. If communication from the End User ceases without notice, after five (5) business days, the Company may, upon notice, close a Support Case due to inactivity on the part of the End User.

(f) The End User agrees to grant access via dedicated secured VPN tunnel, upon receiving a request from the Company for addressing issues reported by the End User. Thus, the Company will have access to the System for a limited period of time in order to reach Problem Resolution. The Company shall have no obligation to provide Support services if the End User does not provide the VPN connection to the System.

(g) The End User agrees to grant access via dedicated secured VPN tunnel, upon the Company's request, for the purpose of Software updates and upgrades or for fixing problems detected during the system operation. Thus, the Company will have access to the System for a limited period of time in order to update/upgrade the System. The Company shall have no obligation to apply any updates/upgrades if the End User does not provide the VPN connection to the System.

(h) The Company shall have no obligation to provide Support services if Internet access / 3G issues occur at the End User's Site.

Exceptions:

In some cases, the Company may not be able to resolve the issue until the access network is stable (for example when the service provider installs firewalls over a period of time or there is a poor 3G coverage or poor Internet access). In these cases, the Problem Resolution period will be paused until the network is stable again.

Opening a support ticket regarding authentication of an inbound roamer identity, will require the customer to provide a valid (activated) IMSI and MSISDN of the specific MNO from the specific country.

Note: System will present targets' information only if such information is available, based on global roaming agreements. SAI (Send Authentication Info) and MSISDN by IMSI, information may not be retrieved if target is hosted by an operator that blocks such queries or in lack of roaming agreements with the telecom gateway.

Technical Support Center:

For End Users covered under a valid Support offering, the Company will provide the following Software Support:

(a) The Company will provide the End User with access to the Company's Technical Support Center 24 hours a day, 7 days a week, 365 days a year.

(b) The Company will provide the End User with assistance in operating, managing and configuring the System as well as resolving any Software technical issues.

(c) The End User is able to submit an unlimited number of support cases by phone, email, and web (Case Management System).

6.1. Support Levels and Support Level activities:

Tier 1 Support – Technical support that is provided by an Engineer trained by the Company. Support activities at this level should include basic software and hardware installations, upgrades, basic troubleshooting, configuration changes and/or operation optimization.

Tier 2 Support – Technical support level that is provided by a Field Service Engineer. Support activities at this level should include all Tier 1 activities, customization management, configuration changes and diagnostics or advanced troubleshooting.

Tier 3 Support – Technical support level that is provided by a Technical Support Specialist. Support activities at this level should include all Tier 1 and Tier 2 activities, in-depth System instructions, advanced diagnostics, and troubleshooting at R&D level. This level of support shall be initiated by a request to the System Support Team.

Activities:

(a) Providing initial client contact

(b) Establishing problem logs and tracking

(c) Providing "how to" support

(d) Determining if an issue is documented

(e) Maintaining configuration knowledge

(f) Working with the End User to duplicate and reproduce problems

(g) Providing internal problem determination and verification

(h) Performing remote diagnosis

Tier 4 Support – Technical support level that is provided by an R&D Engineer. Support activities at this level should include design level consultation and solutions, software R&D diagnostics, and high level of software and hardware fixes and solutions. This level support shall be initiated by a request to the Technical Support Team.

Activities:

(a) Isolating, tracking and fixing operational issues

(b) Working with the End User to duplicate and reproduce problems

(c) Technical evaluation and allocation of defect reports within R&D

(d) Providing system fixes if and when deemed necessary

(e) Performing remote diagnosis

(f) System upgrades

6.2. Severity Levels

Severity Level 1 - Critical Business Impact: Complete System failure in which no field procedure resolves the reported issue. A problem has made a critical application function unusable or unavailable and no workaround exists.

Severity Level 2 - Serious Business Impact: The System is able to work, but is producing major errors in certain requests sent. A problem has made a critical application function unusable or unavailable but a workaround exists.

GA

WT

Severity Level 3 - Minor Business Impact: The system has problems, which do not affect its main functions. A problem has diminished critical or important application functionality or performance but the functionality still performs as specified in the user documentation.

(a) **For Severity Level 1**: the Company's System Support Team and the End User agree to dedicate full time and all the necessary resources to solve the case. Top priority is to restore/improve service, not to debug the problem.

(b) **For Severity Level 2 and 3:** the Company's System Support Team and the End User agree to use their technical resources in order to restore an acceptable level of service or bring relevant information

6.3. Contacting the Technical Support Center

Service Availability: The services of the helpdesk shall be available by way of CRM tool, email, telephone at all times 24 hours a day, 7 days a week.

Report of System failure: The End User shall notify the Company in writing (via e-mail or CRM tool) using the "Customer Support Ticket" form, or by telephone promptly following the discovery of any verifiable and reproducible failure of the System. This SLA does not apply to bug reports or feature requests that are cosmetic or do not otherwise impair the operation of the System. Such bugs reports or feature requests are typically prioritized for handling in some future regularly scheduled product release.

Email Support

The Company's Technical Support Center responds to all support requests sent via email. Generally, this is used as a backup in case the End User is unable to access the Case Management System. Email: helpdesk@globalhelp.support

Telephone Support

The Company's support engineers are available by telephone to receive support requests.

Phone: +44-20-3695-4101

Skype

NOC-HelpDesk

Contact Support via the web portal

The end user can also open a ticket to the Company's Technical Support Center via a dedicated web portal that is connected to a CRM tool. Access is secured with a username and password which the Company will provide.

6.4. Response Time and Resource Commitment

Severity 1

(a) Response Time: 1 hour
(b) Commitment – the Company and the End User will commit the necessary resources around the clock for Problem Resolution to obtain workaround or reduce the severity. Top priority is to

restore/improve service, not to debug the problem. If a workaround could not be provided, the task will be transferred to Supplier's R&D Team for further investigation.

Severity 2

(a) Response Time – 1 hour
(b) Commitment - the Company and the End User will commit the necessary resources during normal business hours for Problem Resolution to obtain workaround or reduce the severity. Top priority is to restore/improve service, not to debug the problem.

Severity 3

(a) Response Time – 4 hours
(b) Commitment – the Company's Technical Support Team and the End User agree to use their technical resources during normal business hours for Problem Resolution to obtain workaround or reduce the severity. Top priority is to restore an acceptable level of service or bring relevant information.

NOTE: In case of Hardware problems, the faulty parts will be shipped and time for shipment will be defined for each specific case. In case of severe software problems, the time for resolution will be defined on a case-by-case basis. The Company will use commercially reasonable efforts to provide Hardware replacement in accordance with the terms set forth in **Section 5 "Hardware Replacement Procedure".**

6.5. Resolution Time and Resource Commitment

Severity 1

(a) Resolution Time: 2 business days
(b) Commitment – the Company and the End User will commit the necessary resources around the clock for Problem Resolution to obtain workaround or reduce the severity. Top priority is to restore/improve service.

Severity 2

(a) Resolution Time – 10 business days
(b) Commitment - the Company and the End User will commit the necessary resources during normal business hours for Problem Resolution to obtain workaround or reduce the severity. Top priority is to restore/improve service.

Severity 3

(c) Resolution Time – the 2nd scheduled SW release
(d) Commitment – the Company's Technical Support Team and the End User agree to use their technical resources during normal business hours for Problem Resolution to resolve the issue in the next scheduled SW release. This will be communicated by the Company to the End user.

7. Clarifications

- The System will extract target 3G keys only if such information is available, based on global roaming agreements. This information may not be retrieved if the target is hosted by an operator that blocks such queries or in lack of roaming agreements with the telecom gateway.
- The System will not extract targets 3G keys from and in specific countries such as the USA and Israel.
- The installation of the system may involve the deployment of a dedicated SS7 telecom gateway at one or more of the mobile operators in the country. The End User shall be responsible for providing access and permissions to the sites where the equipment is to be installed, including the allocation of necessary space, power and ventilation required for the installation of the equipment.
- In case of a cloud-based implementation, i.e., no SS7 gateway implemented at a local telecom operator, billing records of targets may be affected and interception of incoming SMS will be restricted.
- Operating-wise, it is recommended that system queries be used with caution and on highly important cases, this in order to minimize risk of exceeding acceptable threshold in the foreign network for such activity.

The Company reserve the right to end the System's life upon a six months prior notice, with effect not before the lapse of 5 (five) years of a sale of a license to the System to the Reseller and/or the End User. Operation of the System during its life period is conditioned upon timely and full payment of maintenance and support fees during the entire period.

CIVIL COVER SHEET

The JS-CAND 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 in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

WHATSAPP INC., a Delaware corporation, and FACEBOOK, INC., a Delaware corporation

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Cooley LLP, Travis LeBlanc (251097)
101 California Street, 5th floor, San Francisco, CA 94111
415-693-2000

DEFENDANTS

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED

County of Residence of First Listed Defendant ISRAEL
(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)*

CONTRACT

- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 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

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

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

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 & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 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

Brief description of cause:
Computer Fraud and Abuse Act

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $ Permanent Injunction and Damages

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

VIII. RELATED CASE(S), IF ANY *(See instructions)*:

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 10/29/2019

SIGNATURE OF ATTORNEY OF RECORD /s/ Travis LeBlanc