EXHIBIT B

to Declaration of Dana Trexler in Support of Plaintiffs' Opposition to Defendants' Motion for Summary Judgment or Partial Summary Judgment

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC. and META PLATFORMS, INC., Plaintiffs, v. NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED, Defendants.	)	Case No. 19-cv-07123-PJH

EXPERT REPORT OF DANA TREXLER, CPA/CFF

August 30, 2024

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY

I. INTRODUCTION

1. On October 29, 2019, WhatsApp Inc. ("WhatsApp") and Meta Platforms, Inc. ("Meta")[1] (collectively, "Plaintiffs") filed a complaint against NSO Group Technologies Limited ("NSO") and Q Cyber Technologies Limited ("Q Cyber") (collectively, "Defendants") alleging that Defendants used WhatsApp servers to send malware to mobile phones and devices for the purpose of extracting data from other WhatsApp users' target devices and conducting surveillance on those users.[2] As a result of Defendants' alleged conduct, Plaintiffs assert that Defendants violated the Computer Fraud and Abuse Act (in violation of 18 U.S.C. § 1030) and the California Comprehensive Computer Data Access and Fraud Act (in violation of California Penal Code § 502), and breached the terms of service with WhatsApp to which Defendants became bound upon their creation of WhatsApp accounts.[3]

2. This report contains my opinions with respect to the economic remedy amounts, along with the bases for these opinions, to be expressed at trial with respect to the claims filed by Plaintiffs against Defendants.

3. My analyses and opinions assume Defendants will be found liable for the alleged conduct. This assumption is necessary as a basis for my analysis. I have not been engaged to provide opinions on issues relating to liability; therefore, I offer no opinions on liability in this report and do not intend to express any such opinions at trial.

[1] Facebook Inc. changed its name to Meta Platforms Inc. in October 2021. *See* Chris Stokel-Walker, *Why Facebook Changed Its Name to Meta and What is the Metaverse?*, NewScientist (Oct. 21, 2021), https://www.newscientist.com/article/2295438-why-has-facebook-changed-its-name-to-meta-and-what-is-the-metaverse/#:~:text=Here%27s%20everything%20you%20need%20to,as%20Meta%20on%2028%20October. (accessed February 2024); Scott Nover, Why Facebook Changed Its Name, Quartz (Oct. 29, 2021), https://qz.com/2081663/why-facebook-changed-its-name-to-meta (accessed February 2024).

[2] Complaint (Dkt. No.1), ¶ 1.

[3] Complaint (Dkt. No.1), ¶¶ 2, 49-78, Request for Relief section, ¶ 1. The Court subsequently dismissed Plaintiffs' fourth cause of action, Trespass to Chattels. *See* Order Granting in Part and Denying in Part Motion to Dismiss and Denying Motion to Stay Discovery (Dkt. No.111).

II. BASIS FOR ANALYSIS

4. The analysis and opinions in this report are based on the information and documentation identified to date, my education, my experience in performing similar financial analyses and economic damage calculations, documents and testimony in the record, accepted damages methodologies and approaches, and applications of relevant case law.

5. I am a Managing Director at Stout Risius Ross, LLC, an advisory firm that, among other services, provides business, economic, financial, and consulting services to clients in a variety of industries. I lead Stout's national intellectual property disputes and valuations practice. I am a Certified Public Accountant and Certified in Financial Forensics. My education includes a Master in Business Administration from The Wharton School of the University of Pennsylvania and a Bachelor of Science degree in Accounting from Bucknell University. My curriculum vitae is attached as **EXHIBIT A.**

6. In forming my opinions, I considered various documents produced by the parties and non-parties, deposition testimony, and certain legal documents from this case. Specifically, I considered the documents identified throughout this report and the accompanying exhibits. A list of the documents that I considered in forming my opinions is provided in **EXHIBIT B.** The documents and information used in my analysis and report are the types of documents and information upon which experts in my field typically rely when performing such an analysis. In addition to the documents produced by the parties, I considered relevant publicly available information of the type typically relied upon by experts in this field. I also spoke with the following individuals:

- Cortney Padua, Security Engineer within the Cross-Meta Security Detection and Response Team at Meta;[4]
- Michael Scott, Threat Investigator within the Espionage Team at Meta;
- Drew Robinson, Security Engineer at Meta;
- Aashin Guatam, Director of Product Management at WhatsApp;
- Otto Ebeling, former Security Engineer at Meta (UK);

[4] Deposition of Cortney Padua, 13:120-121.

- Jesus Barcons Palau, Software Engineer at Meta;
- Claudiu Gheorghe, former Software Engineering Manager at Meta;
- YuanYuan Wang, Software Engineering Manager at Meta;
- [redacted], Payroll Manager at Meta;
- [redacted], Equity Programs Analyst within the Securities and Disclosure Equity Operations Group at Meta; and
- [redacted], Director in Global Equity Programs at Meta.

7. I understand that discovery is ongoing; therefore, this report is based on information available to date. As discussed in more detail in this report, Defendants have not produced the relevant information sought by Plaintiffs through discovery. Further, depositions of all of the parties' witnesses have yet to be completed as of the date of this report, including that of Sarit Bizinsky Gil, Defendants' designated witness for financial, contract, and other relevant topics.

8. Should additional information, testimony, or documents that affect my analysis or opinions become available after the issuance of my report, I reserve the right to supplement or update my analysis and/or opinions. Additionally, I reserve the right to supplement or update my report based on information, testimony, or documents that have become available within only a short period of time prior to the issuance of this report, as I have had insufficient time to analyze such new information.[5]

9. I reserve the right to prepare supplemental materials such as summaries, graphical exhibits, or charts for trial, as well as to provide opinions and other materials in response to any additional expert opinions.

10. This report is prepared in accordance with the American Institute of Certified Public Accountants ("AICPA") Statement on Standards for Forensic Services. The work performed does not include the performance of an audit, review, or compilation of financial statements in accordance with

[5] On August 26, 2024, four days before the deadline for this report, NSO produced a document (NSO_WHATSAPP_00045858) that appears to include revenue information for certain NSO products. Further, I understand that two of Defendants' witnesses were deposed on August 27, 2024 (Ramon Eshkar) and August 29, 2024 (Yaron Shohat). I have yet to have the opportunity to review these transcripts and incorporate any relevant information into my analysis.

Generally Accepted Auditing Standards ("GAAS") or with attest standards established by the AICPA.

11. My firm is being compensated at a rate of $795 per hour for my time in this matter, regardless of the outcome of this litigation.

III. SUMMARY OF OPINIONS

12. Assuming Defendants are found liable, it is my opinion that the Plaintiffs' expenditure of resources for their response totals $444,719 and a reasonable estimation of Defendants' profits earned in connection with the targeting of 1,500 devices through Defendants' Exploit ranges from $4.3 million to $13.9 million (at a 29% operating profit margin) or $9.5 million to $30.3 million (at a 63% operating profit margin).

Table 1: Summary of Plaintiffs' Claimed Damages and Available Equitable Recoveries[6]

Category	Amount
Plaintiffs' Response Expenses	$444,719
Defendants' Profits Subject to Disgorgement	
At 29% Operating Profit Margin	$4.3 million - $13.9 million
At 63% Operating Profit Margin	$9.5 million - $30.3 million

13. Plaintiffs' response costs reflect labor expenditures related to internal efforts to identify, evaluate and remediate Defendants' improper use of WhatsApp servers and targeting of select WhatsApp users.[7] The estimate for Plaintiffs' response expense is conservative, as the calculations only consider the low-end of employee estimates, exclude certain employees who worked on the response for whom I do not have estimated hours, and while employees expressed that they worked

[6] **EXHIBIT 1.1; EXHIBIT 1.2.** I reserve the right to supplement or amend this report to account for damages to which Plaintiffs assert they are entitled for Defendants' use of Plaintiffs' computers beyond the 1,500 targeted devices discussed in this report. At this time, it is my understanding Defendants have provided insufficient information from which to calculate profits subject to disgorgement that are attributable to Defendants' use of Plaintiffs' computers beyond the 1,500 targeted devises discussed in this report. I understand Plaintiffs reserve any and all rights to seek damages relating to Defendants' use of their servers, including the period during, before, and after 2019.

[7] This report does not calculate or express an opinion on litigation or other legal costs to which Plaintiffs may be entitled and which Plaintiffs may seek to recover from Defendants. I am informed that Plaintiffs do not waive any rights with regard to seeking such costs or others from Defendants.

security patches to stop NSO.[95] On May 13, 2019, Plaintiffs publicly announced their discovery and remediation of the exploit.[96]

47. As a result of Defendants' alleged conduct, Plaintiffs assert the following causes of action against Defendants:[97]

- Violation of the Computer Fraud and Abuse Act (18 U.S.C. §1030);
- Violation of the California Comprehensive Computer Data Access and Fraud Act (California Penal Code §502); and
- Breach of Contract in connection with WhatsApp terms.

VIII. QUANTIFICATION OF PLAINTIFFS' CLAIMED DAMAGES AND AVAILABLE REMEDIES

48. I understand that Plaintiffs seek to recover damages in the form of their actual losses (i.e., compensatory damages) and disgorgement of Defendants' ill-gotten gains. In this instance, the ill-gotten gains reflect the profits that Defendants derived from their alleged conduct. I offer no opinion on whether either remedy is available on Plaintiffs' causes of action, which I understand is a legal question. I have only been asked to calculate Plaintiffs' actual losses and Defendants' ill-gotten gains.

49. As the determination of Plaintiffs' actual losses considers labor cost expenditures, and Defendants' profits reflect those earned from the licensing of NSO's spyware, it is my opinion that these two categories are not duplicative of one another, and therefore, may be additive.

50. Accordingly, I quantify Plaintiffs' actual damages in the form of the expenditure of resources to respond to and remediate Defendants' conduct described in the Complaint and Defendants' profits derived from targeting WhatsApp.

---

[95] *See e.g.*, WA-NSO-00018457-463.
[96] WhatsApp Reveals Major Security Flaw That Could Let Hackers Access Phones, CBS News (May 14, 2019), https://www.cbsnews.com/sanfrancisco/news/whatsapp-reveals-major-security-flaw-that-could-let-hackers-access-phones/ (accessed February 2024).
[97] Complaint (Dkt. No.1), ¶¶ 2, 49-78, Request for Relief section, ¶ 1. Plaintiffs originally alleged that Defendants wrongfully trespassed on Plaintiffs' property, in violation of California law. The Court subsequently dismissed Plaintiffs' fourth cause of action, Trespass to Chattels. *See* Order Granting in Part and Denying in Part Motion to Dismiss and Denying Motion to Stay Discover (Dkt. No.111).

A. PLAINTIFFS' EXPENDITURE OF RESOURCES FOR RESPONSE

51. I understand that on or around April 23, 2019, Plaintiffs began logging activity on servers in connection with a security review.[98] On May 2, 2019, one of WhatsApp's engineers discovered in that logging a malformed and potentially malicious message.[99] Over the following days, WhatsApp and Meta engineers and others investigated the source of the malicious message and its impact on Plaintiffs' systems.[100] Between May 10, 2019 and May 13, 2019, Plaintiffs applied software patches to their relay servers and signaling servers and published a security patch for users' WhatsApp client applications to successful resolve the exploit.[101] On May 13, 2019, Plaintiffs publicly announced their discovery and remediation of the exploit.[102] I understand that Plaintiffs continued to perform ongoing work related to the exploit after the security patch was implemented on May 13, 2019.[103]

52. I understand that Plaintiffs' employees investigated Defendants' Exploit, determined its impact on Plaintiffs' systems, developed and implemented the security patches to resolve the exploit, and performed ongoing work to fully understand the source of the attack, the methods used and full nature of the vulnerability, and the impact on WhatsApp users.[104] As such, the cost incurred by Plaintiffs response to the exploit includes the labor cost associated with certain of Plaintiffs' employees involved in the investigation, remediation, and ongoing efforts surrounding Defendants' alleged conduct, which occurred beginning on or around April 23, 2019, and continued through the latter part of 2019.

53. In the following sections, I describe and quantify select labor hours and associated costs for this work.

[98] *See e.g.*, WA-NSO-00018457-463.
[99] *See* WA-NSO-00017583-604 at 593. S*ee also* WA-NSO-00166464.
[100] *See* WA-NSO-00017583-604 at 593-601. *See also* WA-NSO-00164559-566.
[101] *See* WA-NSO-00017583-604 at 601-603.
[102] https://www.cbsnews.com/sanfrancisco/news/whatsapp-reveals-major-security-flaw-that-could-let-hackers-access-phones/ (accessed February 2024).
[103] Discussion with Cortney Padua, Michael Scott, Drew Robinson, Aashin Guatam, Otto Ebeling, Jesus Palau, Claudiu Gheorghe, and YuanYuan Wang. *See also* WA-NSO-00164559-566.
[104] Discussion with Cortney Padua, Michael Scott, Drew Robinson, Aashin Guatam, Otto Ebeling, Jesus Palau, Claudiu Gheorghe, and YuanYuan Wang. *See also* WA-NSO-00018457-463.

1. Plaintiffs' Employee Labor

54. To determine Plaintiffs' labor costs incurred in connection with investigating Defendants' Exploit, determining its impact on Plaintiffs' systems, developing and implementing the security patch to resolve it, and any associated ongoing work after implementing the security patch, I relied on information from discussions with the following individuals, who were involved with these efforts:

- Cortney Padua, Security Engineer within the Cross-Meta Security Detection and Response Team at Meta;[105]
- Michael Scott, Threat Investigator within the Espionage Team at Meta;
- Drew Robinson, Security Engineer at Meta;
- Aashin Guatam, Director of Product Management at WhatsApp;
- Otto Ebeling, former Security Engineer at Meta (UK);
- Jesus Barcons Palau, Software Engineer at Meta;
- Claudiu Gheorghe, former Software Engineering Manager at Meta; and
- Yuan Yuan Wang, Software Engineering Manager at Meta.

55. My discussions with each of these individuals include an overview of each of their then-in-effect positions and responsibilities, a description of the work they performed in connection with Defendants' Exploit when they performed this work, and an estimation of the amount of time spent in connection with this work. I describe the information represented to me by these individuals in more detail in the following sections.

a. Cortney Padua[106]

56. Cortney Padua is currently a Security Engineer on the Cross-Meta Security Detection and Response Team at Meta.[107] At the time of Defendants' Exploit, Ms. Padua was a Security Engineer on the Computer Emergency Response Team at Meta.

[105] Deposition of Cortney Padua, August 20, 2024, pp. 114, 120-121.
[106] Discussion with Cortney Padua; Deposition of Cortney Padua, August 20, 2024, pp. 24-25, 49-52, 60-61.
[107] Deposition of Cortney Padua, August 20, 2024, pp. 114, 120-121.

57. Ms. Padua described her role in the process as including:[108]

- General coordination and support of the response team and strategizing remediation steps and timelines.[109]
- Reviewing WhatsApp logs to gather evidence of Defendants' Exploit and determine population of targeted users.[110]
- Formatting data contained in these WhatsApp logs for further review and analysis by internal data teams.[111]
- Ongoing review of WhatsApp logs to monitor for potential ongoing exploitation of WhatsApp servers.[112]
- Assisting with eDiscovery preservation of WhatsApp logs obtained during the investigation and remediation.[113]
- Supporting reporting efforts, including drafting summaries and presentations of the subject incident.

58. Ms. Padua estimates that she worked approximately the following number of hours during the noted periods on these tasks:

- May 2 through May 7, 2019 - 24 hours.
- May 8 through May 16, 2019 - 36 hours.
- May 20 through May 28, 2019 - 24 hours.
- Mid-June - 12 hours.

59. Based on my discussion with Ms. Padua, she estimates that she worked a total of 96 hours in relation to Defendants' Exploit. Using Ms. Padua's estimates, 44 hours are allocated to the period May 2 through May 13,[114] and 52 hours are allocated to the period after May 13.[115]

[108] Discussion with Cortney Padua.
[109] See also Deposition of Cortney Padua, August 20, 2024, pp. 24-25, 60-61.
[110] See also Deposition of Cortney Padua, August 20, 2024, pp. 49-52, 60-61.
[111] See also Deposition of Cortney Padua, August 20, 2024, pp. 49-52, 60-61.
[112] See also Deposition of Cortney Padua, August 20, 2024, p. 105.
[113] See also Deposition of Cortney Padua, August 20, 2024, pp. 49-52.
[114] 60 hours during the 11-workday period May 2 through May 16 = 5.5 hours per workday x 8 workdays between May 2 and May 13.
[115] 96 total hours less 44 hours between May 2 and May 13.

b. Michael Scott[116]

60. Michael Scott is currently a Threat Investigator on the Espionage Team at Meta, which was also his title at the time of Defendants' Exploit.

61. Mr. Scott described his role as including:

- Analyzing data to assist in understanding the exploit and determining how it was conducted.
- Reviewing and analyzing WhatsApp logs to obtain information such as IP addresses and phone numbers that could help identify targeted WhatsApp users. The identification of targeted users also considered research of publicly available information and other profile information maintained by Meta (e.g., Facebook and Instagram profile information).
- Efforts related to determining the source of the exploit, including cross referencing current information from WhatsApp logs (e.g., IP addresses, domains, and phone numbers) with previously identified information for suspected "test accounts" used by attackers prior to the exploit, which included suspected accounts associated with NSO. Identifying the source of the exploit and related accounts to assist in disabling accounts and preventing those accounts from accessing WhatsApp.
- Attempting to map attackers with victims, including the determination of countries of origin for attacker accounts.

62. Mr. Scott represented that in relation to Defendants' Exploit, he spent nearly all his working time on these efforts over a 2 to 3-month period beginning in or around April/May 2019. Mr. Scott further stated that ongoing work continued for "months and months," but did not provide an estimate of the portion of his time spent on these ongoing efforts. Using the low end of Mr. Scott's estimate (i.e., 2 months), 64 hours are allocated to the period May 2 through May 13,[117] and 256 hours are allocated to the period after May 13[118] in relation to Defendants' Exploit.

c. Drew Robinson[119]

63. Drew Robinson is currently a Security Engineer at Meta. At the time of Defendants' Exploit, Mr. Robinson was a Security Investigator at Meta.

[116] Discussion with Michael Scott.
[117] 8 hours per workday x 8 workdays between May 2 and May 13.
[118] 320 hours over a 2-month period (160 work hours in a month [40 hours per week x 4 weeks] x 2 months) less 64 hours between May 2 and May 13.
[119] Discussion with Drew Robinson.

64. Mr. Robinson described his role as including:

- Serving as the "on call" for malware analysis and working with WhatsApp engineers to immediately analyze WhatsApp logs to evaluate the "payload" used to deliver the malware to victims.
- Performing various analyses of WhatsApp logs and server information to extract the payloads that had been deployed to help identify the source of the payload (i.e., the orchestrator of the attack).
- Assisting with identification of targeted WhatsApp users and map them back to the malware users. This included analyzing country codes associated with targeted accounts and the nature of the accounts (based in part on publicly available information and Facebook and Instagram profile information).
- Assisting WhatsApp engineers in developing and deploying the security patch.
- Ongoing monitoring for future attacks/exploits and further analysis of ways that NSO was targeting Plaintiffs' services.
- Continued assistance with victim identification.
- Supporting Plaintiffs' legal department and responding to requests for information.

65. Mr. Robinson represented that he initially worked full time on the exploit for 3 weeks up to the deployment of the security patch, which he conservatively estimated to approximate 120 hours. Mr. Robinson estimated that he worked another 150-200 hours after the security patch was implemented. Using Mr. Robinson's estimates, 64 hours are allocated to the period May 2 through May 13,[120] and 150 hours are allocated to the period after May 13 in relation to Defendants' Exploit.

d. Aashin Guatam[121]

66. Aashin Guatam is currently a Director of Product Management at WhatsApp. At the time of Defendants' Exploit, Mr. Guatam was a Director of Customer Operations at WhatsApp.

67. Mr. Guatam described his role as including:

[120] 8 hours per workday x 8 workdays between May 2 and May 13.
[121] Discussion with Aashin Guatam.

- Overall project management of the plan implemented by Plaintiffs to resolve Defendants' Exploit, including post-fix identification of and communication with targeted users, external communication strategy, and legal pursuits.

- Working with and guiding technical teams, operations teams, legal teams, and others to understand the attack and identify the victims of the exploit. This included identifying the targeted accounts and mapping them to the real-life users. The accounts were mapped to real-life users using information from WhatsApp accounts, associated social media accounts, and other publicly available information.

- Developing a victim outreach strategy and working with technical teams, operations teams, legal teams, and others to notify the identified victims of the exploit.

68. Mr. Guatam represented to me that he spent, on average, 50% of his working hours from May/June to November 2019 working on this matter. As such, I have considered the low end of Mr. Guatam's estimate (i.e., beginning in June) that he worked 480 hours (6 months [June through November] multiplied by 160 working hours per month multiplied by 50%). Using Mr. Guatam's estimate, all 480 hours are allocated to the period after May 13 in relation to Defendants' Exploit.

e. Otto Ebeling[122]

69. Otto Ebeling currently owns a cyber security consulting company that is sometimes contracted by Plaintiffs. At the time of responding to Defendants' Exploit, Mr. Ebeling was a Security Engineer at Meta, based in the United Kingdom.

70. Mr. Ebeling described his role as including:

- Investigating initial reports relayed to him from WhatsApp engineers to ascertain if a vulnerability existed. This included determining whether the suspicious activity was benign or malicious.

- Understanding Defendants' Exploit and how it worked.

- Determining how to respond to and prevent Defendants' Exploit. Mr. Ebeling consulted with WhatsApp engineers that ultimately created and implemented the security patch.

- Monitoring applicable information to confirm the security patches were working as intended after they were implemented by Plaintiffs' employees.

[122] Discussion with Otto Ebeling.

- Determining if Defendants were exploiting any other unknown vulnerabilities. This included reviewing and analyzing certain software code.

71. Mr. Ebeling represented to me that during the initial remediation work of resolving Defendants' Exploit, he spent all his working hours for 3 weeks on this project. Mr. Ebeling also informed me that he spent one-third (33%) to one-half (50%) of his working time for the second half of 2019 working on ongoing matters associated with Defendants' Exploit. Using Mr. Ebeling's estimates, 64 hours are allocated to the period May 2 through May 13,[123] and 320 hours[124] are allocated to the period after May 13 in relation to Defendants' Exploit.

f. Jesus Barcons Palau[125]

72. Jesus Barcons Palau is currently a Software Engineer at Meta, which was also his title at the time of Defendants' Exploit in May 2019.

73. Mr. Palau described his role as including:

- Consulting with security professionals to investigate abnormal "stanzas"[126] in data passing through WhatsApp servers. This included identifying and investigating stanzas that did not conform with specifications established by WhatsApp. After certain abnormal stanzas were identified, Mr. Palau worked to implement processes to detect other non-conforming and potentially malicious stanzas in data.
- Implementing code to detect malicious stanzas not adhering to WhatsApp specifications.
- Implementing measures to assure that invalid stanzas were blocked from WhatsApp servers.

74. Mr. Palau informed me that during the initial response efforts, he spent all his working time, and additional overtime hours, on this project. Mr. Palau represented to me that he spent more than 100% of his working hours from April 29 through May 10 on response efforts. Using Mr. Palau's estimates, 56 hours are allocated to the period May 2 through May 10[127] in relation to Defendants' Exploit.

[123] 8 hours per workday x 8 workdays between May 2 and May 13.
[124] 6 months multiplied by 160 working hours in a month multiplied by 1/3 of his working time.
[125] Discussion with Jesus Palau.
[126] Stanza is "a general term in WhatsApp for metadata -- for a type of metadata that is sent from a client to a server." Claudiu Gheorghe Deposition, 24:19-24.
[127] 8 hours per workday x 7 workdays between May 2 and May 10.

g. Claudiu Gheorghe[128]

75. Claudiu Gheorghe was a Software Engineering Manager at Meta at the time of Defendants' Exploit in May 2019.

76. Mr. Gheorghe described his role as including:

- Coordinating the investigation and remediation of Defendants' Exploit. Mr. Gheorghe orchestrated efforts among engineering teams, security teams, and legal teams.
- Supervising Meta engineers to execute the investigation and remediation of Defendants' Exploit. This included effectively allocating staffing resources to execute this project. Mr. Gheorghe performed a managerial role in connection with leading coordination for the investigation and remediation of Defendants' Exploit.
- Identifying victims of Defendants' Exploit.
- Assisting in drafting a white paper regarding Defendants' Exploit.

77. Mr. Gheorghe represented to me that during the initial remediation work of resolving Defendants' Exploit, he spent all his working hours from May 2, 2019 through May 13, 2019 on this project. After the patch was implemented on May 13, 2019, Mr. Gheorghe informed me that he spent 50% of his time on this project for two more weeks. Using Mr. Gheorghe's estimates, 64 hours are allocated to the period May 2 through May 13,[129] and 40 hours are allocated to the period after May 13[130] in relation to Defendants' Exploit.

h. YuanYuan Wang[131]

78. YuanYuan Wang is currently a Software Engineering Manager at Meta, which was also his title at the time of Defendants' Exploit in May 2019.

79. Mr. Wang described his role as including:

- Confirming that the exploit was occurring. This included identifying abnormal patterns through his knowledge of the WhatsApp architecture.

[128] Discussion with Claudiu Gheorghe.
[129] 8 hours per workday x 8 workdays between May 2 and May 13.
[130] 80 hours over a 2-week period (2 weeks x 40 hours per week) x 50%.
[131] Discussion with YuanYuan Wang.

- Organizing and providing applicable information regarding Defendants' Exploit to security teams at Meta.
- Consulting with security teams at Meta to identify the software code permitting Defendants' Exploit.
- Understanding the software code relevant to Defendants' Exploit.
- Consulting with security teams at Meta to improve and secure the applicable software code. This fixed the software code permitting Defendants' Exploit.

80. Mr. Wang represented to me that during the initial remediation work of resolving Defendants' Exploit, he spent all his working hours from May 2, 2019 through May 13, 2019 on this project. Using Mr. Wang's estimate, 64 hours are allocated to the period May 2 through May 13[132] in relation to Defendants' Exploit.

i. Other Employees Identified by Claudiu Gheorghe[133]

81. In addition to the discussions I had with the above-noted individuals, Claudiu Gheorghe identified 14 other Meta professionals that participated in the investigation and response efforts.[134] As discussed, Mr. Gheorghe was a Software Engineering Manager at Meta who performed a managerial role leading coordination across multiple teams in connection with addressing Defendants' Exploit in May 2019.

82. Mr. Gheorghe provided descriptions of roles and estimates of hours worked for each of the Meta employees he identified as participating in the investigation and response efforts from May 2, 2019 through May 13, 2019. This is reflected in **EXHIBIT 2.2** to my report.

2. Plaintiffs' Employee Labor Cost

83. After identifying the employees involved in responding to Defendants' Exploit, and their respective estimated labor hours, I determined the cost of this labor. To determine the cost of labor of each applicable employee, I multiplied each applicable employee's burdened labor rate by the number of hours worked on responding to Defendants' Exploit.

[132] 8 hours per workday x 8 workdays between May 2 and May 13.
[133] Discussion with Claudiu Gheorghe.
[134] **EXHIBIT 2.2.**

84. The calculation of an employee's burdened labor rate not only considers the employee's salary, but also considers other expenditures paid by an employer to, or on behalf of, an employee. These additional expenditures can be paid directly to an employee (e.g., performance bonus or retirement contributions) or paid on behalf of an employee (e.g., the employer's share of healthcare insurance premiums or payroll taxes). In addition to base salary, the inclusion of an employer's additional expenditures to, or on behalf of, an employee reflects the employer's total economic cost incurred in connection with the subject employee's time.

85. To calculate each employee's burdened labor rate, I relied on data provided by Plaintiffs detailing payroll information for specific employees which included wages, employee and employer payroll taxes, and certain employer-paid benefits. I also obtained employee bonus information and the amount of employer-paid health benefits. For purposes of determining a compensation rate for individual employees, I considered the following costs incurred by Plaintiffs:

- Salary
- Performance bonus
- Employer payroll taxes
- Employer portion of health benefits
- Restricted Stock Unit ("RSU") grants

86. As detailed in **EXHIBIT 3.1**, I considered the above amounts and determined an hourly-equivalent compensation rate for each of the individuals discussed in the preceding section. I determined Plaintiffs' relevant expenditures by multiplying each applicable employee's hours spent on resolving Defendants' Exploit and for related ongoing work by their burdened labor rate. As summarized in the following table, Plaintiffs' expenditures to respond to Defendants' Exploit total $444,719.

Table 3: Plaintiffs' Labor Expenses to Respond to Defendants' Exploit [135]

Employee Name	2019 Title	Hours Worked	Hourly Rate	Cost of Labor
Cortney Padua	Security Engineer	96	$112.51	$10,801
Michael Scott	Threat Investigator	320	$194.28	$62,169
Drew Robinson	Security Investigator	214	$107.64	$23,035
Aashin Guatam	Director of Customer Ops.	480	$195.38	$93,785
Otto Ebeling	Security Engineer	384	$149.86	$57,545
Jesus Palau	Software Engineer	56	$249.03	$13,946
Claudiu Gheorghe	Software Engineering Manager	104	$404.25	$42,042
YuanYuan Wang	Software Engineering Manager	64	$561.38	$35,928
			Cost of Labor	**$339,250**
			Cost of Labor (Additional Employees Identified by Mr. Gheorghe)	**$105,469**
			Total Cost of Labor	**$444,719**

87. The estimate included in Table 3 is conservative, as the calculations only consider the low-end of employee estimates, exclude certain employees who worked on the response for whom I do not have estimated hours, and while employees expressed that they worked extended hours and weekends, I do not include such extended hours and weekends in my calculations.

88. While these individuals were salaried employees and were not paid on an hourly basis, the hourly equivalent labor rate provides a means to determine the cost of their respective time to Plaintiffs with respect to responding to Defendants' Exploit. While some of these individuals perform security-related tasks in the ordinary course of their employment by Plaintiffs, they would have directed this time to other efforts in the absence of Defendants' alleged conduct. Accordingly, these efforts and associated cost are reflective of an "opportunity cost" to Plaintiffs. Further, as this was a required effort in light of Defendants' Exploit, in the absence of these employees, Plaintiffs would have needed to expend resources to obtain these types of services from third parties.

B. Defendants' Ill-Gotten Gains Subject to Disgorgement

89. In this instance, Defendants' ill-gotten gains subject to disgorgement reflect the profit that Defendants derived from their unauthorized access to Plaintiffs' systems, including the use of Defendants' Exploit. I understand that Plaintiffs allege that Defendants' Exploit for the WhatsApp Service was the Android zero-click installation vector for Pegasus or similar spyware in use from

[135] **Exhibits 1.1, 2.1, and 2.2.**

at least January 1, 2018 through May 13, 2019, and that both Defendants' development and sale of that exploit violated its Terms of Service and federal and state law. Accordingly, I estimate Defendants' ill-gotten gains resulting from the development and licensing of Pegasus with the Android zero-click feature, and any other spyware targeting Plaintiffs' systems based on the information available to date.

90. As discussed in further detail, Plaintiffs assert that Defendants have not produced all relevant information, and depositions of Defendants' witnesses have only recently occurred[136] or are scheduled to occur after the date of this report. Accordingly, I reserve the right to update my analysis based on such information.

91. Specifically, I understand that Plaintiffs requested from Defendants the information to evaluate Defendants' ill-gotten gains from targeting Plaintiffs' systems. As of the date of this report, I understand that Defendants have not produced certain financial information, other than the materials cited in this report (and in Exhibit B to this report), relevant to an assessment of Defendants' ill-gotten gains.

92. Given the absence of certain information requested from Defendants, my assessment of Defendants' profits recognized in conjunction with the alleged conduct relies on the documents produced to date and reasonable assumptions regarding certain information contained in those documents. Additional documents produced by Defendants (or other parties) and future deposition testimony may impact my analysis, assumptions, and conclusions.

93. The following sections address my determination of Defendants' ill-gotten gains subject to disgorgement based on the information reasonably available to me to date.

1. Total Reported Revenue from the Sale and License of the Pegasus Product

94. As an initial matter, I consider the reported revenues for Pegasus contained in certain financial information produced to date. In 2018, Pegasus generated approximately $183 million in

[136] Given the timing of Defendants' depositions, I have not fully evaluated the testimony or its impact on my analysis.

Table 8: Profit from Defendants' Exploit[188]

Category	Devices	$ Fee/ Device	Revenue	Op. Profit 29%	Op. Profit 63%
Basic Only	1,500	$120,000	$180,000,000	$52,172,447	$113,548,740
Basic and Additional Concurrent Targets (Excl. Add'l Concurrent Targets Only)	1,500	$32,000	$48,000,000	$13,912,652	$30,279,664
Additional Concurrent Targets Only	1,500	$10,000	$15,000,000	$4,347,704	$9,462,395

123. As noted previously, the consideration of per-device fees that take into account the lower prices of "additional concurrent targets" is a more conservative approach to reflect the nature of concurrent licenses and the reduction of the per-device fee as more devices are targeted. Accordingly, based on the information contained in Table 8, a reasonable estimation of Defendants' profits earned in connection with the targeting of 1,500 devices through Defendants' Exploit ranges from $4.3 million to $13.9 million (at a 29% operating profit margin) or $9.5 million to $30.3 million (at a 63% operating profit margin).

C. DEFENDANTS' USE OF PLAINTIFFS' SYSTEMS

124. Counsel for Plaintiffs asked me to determine whether the use of Plaintiffs' systems for purposes of Defendants' Exploit was worth more than $5,000 in one year to Defendants or their customers. To do so, I consider the customer revenue amounts related to the covert-Android version of Pegasus as a reasonable proxy to quantify this amount, based on the limited information produced by Defendants to date.

125. I first consider that, in a March 2019 "Q&A" document, the Defendants state, "Pricing depends on the product, number of capabilities and number of licenses. On average for the mobile endpoint products, prices range mainly between $1m and $10m per license, i.e., target/endpoint."[189] Also of note, this range is the amount for one license, and Defendants benefit by being able to have multiple licensees to its software, including Pegasus, resulting in a multiplier effect of licensing revenues to Defendants.

[188] **EXHIBITS 4 AND 4.1.**
[189] WA-NSO-00074412-414 at 413-414.

126. I next consider that the Defendants produced a document which appears to identify customer revenue amounts. Analysis of this document appears to enable the identification of revenue related to the covert-Android version of Pegasus, specifically, the upsell data contained therein.[190] Table 9 summarizes the annual revenue from three upsell transactions for the covert-Android Pegasus product.

TABLE 9: "COVERT ANDROID"- ONLY "UPSELL" LINE ITEMS ANNUAL REVENUES BASED ON FIRST FOUR QUARTERS[191]

Account No.	Start Qtr.	End Qtr.	Annual First Year Revenue
Acc-04	Q3 2018	Q2 2019	$6,835,000
Acc-06[192]	Q1 2019	Q4 2019	1,412,000
Acc-57	Q3 2018	Q2 2019	5,630,000
Total			$13,877,000

127. From this data, it is my opinion that the use of Plaintiffs' systems for purposes of Defendants' Exploit was worth $13,877,00 for these three accounts[193] alone, which exceeds $5,000 in one year.

* * * * * *

[190] *See* NSO_WHATSAPP_00045858.
[191] NSO_WHATSAPP_00045858.
[192] Only considering "No" responses for other capabilities (i.e., excluding "(blanks)") results in this line item being the only "Covert Android"-Only "Upsell" Line Item.
[193] Based solely on "Upsell" transactions of "Covert-Android."

128. The procedures performed were limited to those described herein based on the documents provided to date and other information obtained. Information obtained after the date of this report, or within a short period of time prior to its issuance, may affect this analysis and this effect may be material. If requested, I will update my analysis.

129. My procedures were performed solely with respect to the above referenced litigation. This report is not to be reproduced, distributed, disclosed, or used for any other purpose.

STOUT

Dana M. Trexler, CPA/CFF August 30, 2024

EXHIBIT C

to Declaration of Dana Trexler in Support of Plaintiffs' Opposition to Defendants' Motion for Summary Judgment or Partial Summary Judgment

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC. and META PLATFORMS, INC.,	)	
Plaintiffs,	)	
v.	)	Case No. 19-cv-07123-PJH
NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,	)	
Defendants.	)	

SUPPLEMENTAL EXPERT REPORT OF DANA TREXLER, CPA/CFF

September 21, 2024

HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY

I. INTRODUCTION

1. On October 29, 2019, WhatsApp Inc. ("WhatsApp") and Meta Platforms, Inc. ("Meta")[1] (collectively, "Plaintiffs") filed a complaint against NSO Group Technologies Limited ("NSO") and Q Cyber Technologies Limited ("Q Cyber") (collectively, "Defendants") alleging that Defendants used WhatsApp servers to send malware to mobile phones and devices for the purpose of extracting data from other WhatsApp users' target devices and conducting surveillance on those users.[2] As a result of Defendants' alleged conduct, Plaintiffs assert that Defendants violated the Computer Fraud and Abuse Act (in violation of 18 U.S.C. § 1030) and the California Comprehensive Computer Data Access and Fraud Act (in violation of California Penal Code § 502), and breached the terms of service with WhatsApp to which Defendants became bound upon their creation of WhatsApp accounts.[3]

2. On August 30, 2024, I submitted an expert report in this matter ("Initial Report"). I have been asked by Counsel to supplement my Initial Report based on information that became available after the issuance of my Initial Report, including testimony from the September 6, 2024 deposition of Sarit Bizinsky Gil ("Gil Deposition"). This report supplements, and should be read in conjunction with, the Initial Report. The Initial Report is incorporated herein by reference.

II. BASIS FOR ANALYSIS

3. The basis for my analysis and opinions in this report are the same as those stated in the Initial Report.[4] In addition to the information considered in the Initial Report (as identified in **EXHIBIT B** thereto), I also consider additional information since the date of that report, as identified in **SUPPLEMENTAL EXHIBIT B**.

[1] Facebook Inc. changed its name to Meta Platforms Inc. in October 2021. *See* Chris Stokel-Walker, *Why Facebook Changed Its Name to Meta and What is the Metaverse?*, NewScientist (Oct. 21, 2021), https://www.newscientist.com/article/2295438-why-has-facebook-changed-its-name-to-meta-and-what-is-the-metaverse/#:~:text=Here%27s%20everything%20you%20need%20to,as%20Meta%20on%2028%20October. (accessed February 2024); Scott Nover, Why Facebook Changed Its Name, Quartz (Oct. 29, 2021), https://qz.com/2081663/why-facebook-changed-its-name-to-meta (accessed February 2024).
[2] Complaint (Dkt. No.1), ¶ 1.
[3] Complaint (Dkt. No.1), ¶¶ 2, 49-78, Request for Relief section, ¶ 1. The Court subsequently dismissed Plaintiffs' fourth cause of action, Trespass to Chattels. *See* Order Granting in Part and Denying in Part Motion to Dismiss and Denying Motion to Stay Discovery (Dkt. No.111).
[4] My curriculum vitae has not changed since my Initial Report, which is attached as **EXHIBIT A** thereto.

4. Should additional information, testimony, or documents that affect my analysis or opinions become available after the issuance of this report, I reserve the right to supplement or update my analysis and/or opinions. I reserve the right to prepare supplemental materials such as summaries, graphical exhibits, or charts for trial, as well as to provide opinions and other materials in response to any additional expert opinions.

III. SUMMARY OF OPINIONS

5. Assuming Defendants are found liable, it is my opinion that a conservative estimate of the Plaintiffs' expenditure of resources for their response totals $444,719.[5] My opinion and the accompanying methodology I used to calculate this figure are discussed in my Initial Report.

6. Based on the limited information available to me at the time of my Initial Report, I set forth that a reasonable estimation of Defendants' profits earned specifically in connection with the targeting of the 1,500 devices through Defendants' Exploit[6] ranges from $4.3 million to $13.9 million (at a 29% operating profit margin) or $9.5 million to $30.3 million (at a 63% operating profit margin).[7] Given that Defendants produced NSO_WHATSAPP_ 00045858 ("Defendants' Spreadsheet") and Ms. Sarit Bizinsky Gil has now testified (as Defendants' corporate representative) that this document contains the revenue amounts for customer contracts which include at least the Covert Android vector, it is my opinion that Defendants' Spreadsheet, and the related testimony, provides a more detailed basis upon which to calculate Defendants' profits, than the limited information available to me at the date of the Initial Report.[8,9]

7. Based on adjustments I made to Defendants' Spreadsheet, as discussed herein, it is my opinion that a reasonable estimation of Defendants' profits earned in connection with Defendants' Exploit ranges between at least $21.3 million to $40.2 million, which includes adjustments for the profit

[5] Initial Report, ¶ 12.
[6] The use of "Defendants' Exploit" herein is consistent with the use of this term in the Initial Report. *See e.g.*, Initial Report, ¶¶ 44-45.
[7] Initial Report, ¶ 12.
[8] I understand that during the period generally covered by Defendants' Spreadsheet (Q2 2018 through Q2 2020), Defendants did not have zero-click/covert installation vectors for Android other than those that were activated through WhatsApp. *See e.g.*, Deposition of Tamir Gazneli, September 4, 2024, pp. 39, 67-68, and 103.
[9] As noted throughout this report, there is additional information that Defendants have not yet produced, which would be useful for the calculation of Defendants' profits; therefore, I reserve the right to update the opinions and analyses expressed herein, if asked, if additional information is received.

margins and reductions to revenue made by Defendants for time (i.e., availability of the Covert Android vector) and maintenance.[10] Given the lack of information provided by Defendants to assess the value of the Covert Android vector relative to other vectors (Triggered Android, Triggered iOS, and Covert iOS), Defendants' subject revenues and profits could exceed even these revised amounts calculated herein.

8. My opinions are summarized in the table below.

Table 1: Summary of Plaintiffs' Claimed Damages and Available Equitable Recoveries[11]

Category	Amount
Plaintiffs' Response Expenses	$444,719
Defendants' Profits Subject to Disgorgement – Defendants' Spreadsheet Approach	
Adjusted Profit Margin	$5.5 million - $10.5 million
Adjusted Profit Margin; Adjusted Revenue for Time	$17.3 million - $32.6 million
Adjusted Profit Margin; Adjusted Revenue for Time and Maintenance	$21.3 million - $40.2 million

9. I understand that there are certain legal arguments advanced by counsel for the Plaintiffs, wherein the Plaintiffs posit that certain costs may not be deductible from Defendants' revenues generated by Defendants' Exploit, because those costs and related activities themselves involved conduct that is the subject of Plaintiff's claims. To the extent the fact finder needs to identify the revenues or certain expenses attributed to Defendants' Exploit, this information can be found in **SUPPLEMENTAL EXHIBITS 1, 2, AND 3** and **INITIAL REPORT EXHIBITS 4, 5.1, AND 5.1.1**.

10. Counsel for Plaintiffs also asked me to determine whether the use of Plaintiffs' systems for purposes of Defendants' Exploit was worth more than $5,000 in one year to NSO or its customers. It is my opinion that the use of Plaintiffs' systems for purposes of Defendants' Exploit was worth $13,877,000 for three accounts alone,[12,13] which exceeds $5,000 in one year. My opinion and the accompanying methodology I used to calculate this figure is discussed in my Initial Report.

[10] **SUPPLEMENTAL EXHIBIT 1.**
[11] See my Initial Report, Table 1; **SUPPLEMENTAL EXHIBITS 1, 2, AND 3**.
[12] Based solely on "Upsell" transactions of "Covert-Android."
[13] Initial Report, ¶¶ 126-127.

IV. SUPPLEMENTAL ANALYSES AND OPINIONS

11. On September 6, 2024, after my Initial Report was served, Sarit Bizinsky Gil, Vice President of Global Business Operations at Q Cyber, was deposed.[14] Ms. Bizinsky Gil testified regarding an Excel spreadsheet produced by Defendants and prepared by Ms. Bizinsky Gil (NSO_WHATSAPP_00045858),[15] which purports to set forth Pegasus (and other products) contract revenues and purported profits during the period Q2 2018 through Q2 2020 ("Defendants' Spreadsheet"). Besides quarterly revenue amounts, other information includes a revenue classification (e.g., upsell, maintenance), Defendants' own allocation of revenue to Defendants' Exploit, and a calculation of purported profits on the allocated revenues.

12. It is my understanding that Defendants' Spreadsheet was prepared specifically for this litigation, based in part on instructions from counsel, and is not a document prepared or maintained in the ordinary course of Defendants' business.[16] Ms. Bizinsky Gil testified to the meaning of the information contained within the columns and rows of Defendants' Spreadsheet and provided an overview of the methodology employed by Defendants in preparing Defendants' Spreadsheet and their assessment of the revenue and profit amounts attributable to Defendants' Exploit reflected in it. Defendants have not produced any of the contracts or other underlying information on which Defendants' Spreadsheet is based.

13. Even assuming the revenue and contract information reported in Defendants' Spreadsheet is accurate, based on my analysis of Defendants' Spreadsheet, Ms. Bizinsky Gil's testimony, and other materials produced by Defendants, as well as my experience and training, I believe the calculations of revenues and profits earned through Defendants' Exploit that appear in Defendants' Spreadsheet require adjustment for the reasons I explain in the remainder of this section.[17]

[14] Deposition of Sarit Bizinsky Gil, September 6, 2024, pp. 12, 16.
[15] Deposition of Sarit Bizinsky Gil, September 6, 2024, p. 158.
[16] Deposition of Sarit Bizinsky Gil, September 6, 2024, pp. 158-160.
[17] *E.g.*, Ms. Bizinsky Gil testified that she used a spreadsheet from Defendants' finance department with customer contract information (Deposition of Sarit Bizinsky Gil, September 6, 2024, pp. 161-162), customer deal information from the CRM system (Deposition of Sarit Bizinsky Gil, September 6, 2024, p. 166), and customer contracts (Deposition of Sarit Bizinsky Gil, September 6, 2024, p. 187).

Spreadsheet to not limit revenues to only the days when the Covert Android vector was allegedly operational, and adjusting revenue to include all maintenance revenues results in calculated profits of $21.3 million (using operating profit margin) and $40.2 million (using operating profit margin excluding research and development expenses),[94] compared to the $72,000 calculated by Defendants.[95] It is my opinion that all of these adjustments are reasonable and appropriate for the reasons explained above. Accordingly, it is my opinion that a reasonable estimation of Defendants' profits earned in connection with Defendants' Exploit ranges between at least $21.3 million to $40.2 million.

48. **Adjusted Revenue for Time and Maintenance:** Adjusting revenue presented in Defendants' Spreadsheet to not limit revenues to only the days when the Covert Android vector was allegedly operational, and to include all maintenance revenues, results in calculated revenues of $61.7 million (this amount is not reduced by expenses).[96] This adjusted revenue amount is compared to the approximately $16.1 million of revenue estimated by Defendants.[97]

* * * * * *

49. The procedures performed were limited to those described herein based on the documents provided to date and other information obtained. Information obtained after the date of this report, or within a short period of time prior to its issuance, may affect this analysis and this effect may be material. If requested, I will update my analysis.

50. My procedures were performed solely with respect to the above referenced litigation. This report is not to be reproduced, distributed, disclosed, or used for any other purpose.

STOUT

Dana M. Trexler, CPA/CFF September 21, 2024

[94] **SUPPLEMENTAL EXHIBIT 1**.
[95] See NSO_WHATSAPP_00045858.
[96] **SUPPLEMENTAL EXHIBIT 1**.
[97] *See* NSO_WHATSAPP_00045858.

Supplemental Exhibit 1

WhatsApp, et al. v. NSO Group, et al.

Profits Subject to Disgorgement Based on Presented Pegasus "Final Relevant Revenue" Excluding Time and Maintenance Adjustments (Q2 2018 - Q2 2020)

Supplemental Exhibit 1

			Q2 - Q4 2018	2019	Q1 - Q2 2020	Q2 2018 - Q2 2020
1	Presented Pegasus "Final Relevant Revenue" Excluding Time and Maintenance Adjustments	[1]	$ 19,439,947	$ 31,055,220	$ 11,213,759	**$ 61,708,926**
2	NSO Group Technologies Ltd. Operating Margin	[2]	44.0%	29.0%	33.5%	**34.5%**
3	**Profits Subject to Disgorgement**		**$ 8,552,765**	**$ 9,001,260**	**$ 3,760,462**	**$ 21,314,487**

			Q2 - Q4 2018	2019	Q1 - Q2 2020	Q2 2018 - Q2 2020
4	Presented Pegasus "Final Relevant Revenue" Excluding Time and Maintenance Adjustments	[1]	$ 19,439,947	$ 31,055,220	$ 11,213,759	**$ 61,708,926**
5	NSO Group Technologies Ltd. Operating Margin (Excluding R&D Expenses)	[3]	67.9%	63.1%	66.4%	**65.2%**
6	**Profits Subject to Disgorgement**		**$ 13,207,238**	**$ 19,590,451**	**$ 7,446,204**	**$ 40,243,892**

[1] Supplemental Exhibit 1.1.

[2] See my Initial Report, Exhibit 5.1.

[3] See my Initial Report, Exhibit 5.1.1.

WhatsApp, et al. v. NSO Group, et al.
Presented Pegasus "Final Relevant Revenue" Excluding Time and Maintenance Adjustments (Q2 2018 - Q2 2020)
Supplemental Exhibit 1.1

	Account No.	Q2 - Q4 2018	2019	Q1 - Q2 2020	Q2 2018 - Q2 2020
1	Acc-01	$ -	$ -	$ -	$ -
2	Acc-02	$ -	$ -	$ -	$ -
3	Acc-03	$ 933,500	$ 1,402,390	$ 660,831	$ 2,996,721
4	Acc-04	$ 6,069,231	$ 2,410,849	$ 763,671	$ 9,243,751
5	Acc-05	$ -	$ 604,000	$ 633,306	$ 1,237,306
6	Acc-06	$ -	$ 1,412,348	$ 180,620	$ 1,592,969
7	Acc-07	$ -	$ -	$ 807,022	$ 807,022
8	Acc-08	$ -	$ -	$ -	$ -
9	Acc-09	$ -	$ -	$ -	$ -
10	Acc-10	$ 455,792	$ 1,055,518	$ 545,751	$ 2,057,060
11	Acc-12	$ -	$ -	$ -	$ -
12	Acc-13	$ 54,963	$ 69,431	$ 35,709	$ 160,102
13	Acc-14	$ -	$ 60,706	$ 37,238	$ 97,944
14	Acc-16	$ -	$ 693,527	$ 87,913	$ 781,440
15	Acc-18	$ -	$ 945,151	$ 54,849	$ 1,000,000
16	Acc-19	$ -	$ -	$ -	$ -
17	Acc-20	$ -	$ -	$ -	$ -
18	Acc-21	$ 990,725	$ 1,256,314	$ 654,452	$ 2,901,491
19	Acc-22	$ -	$ -	$ -	$ -
20	Acc-23	$ -	$ 1,570,849	$ 189,981	$ 1,760,831
21	Acc-24	$ -	$ -	$ -	$ -
22	Acc-25	$ -	$ -	$ -	$ -
23	Acc-26	$ 779,683	$ 188,844	$ 74,452	$ 1,042,979
24	Acc-27	$ -	$ 917,783	$ 105,149	$ 1,022,932
25	Acc-29	$ -	$ 1,593,128	$ 212,159	$ 1,805,287
26	Acc-31	$ 169,166	$ 200,592	$ 100,830	$ 470,588
27	Acc-32	$ -	$ 1,446,189	$ 296,739	$ 1,742,928
28	Acc-33	$ 694,000	$ 567,096	$ 431,750	$ 1,692,846
29	Acc-34	$ 211,916	$ 21,577	$ -	$ 233,493
30	Acc-37	$ -	$ -	$ -	$ -
31	Acc-38	$ -	$ -	$ -	$ -
32	Acc-39	$ -	$ 479,698	$ 38,702	$ 518,400
33	Acc-40	$ 442,500	$ 180,096	$ 176,168	$ 798,764
34	Acc-41	$ -	$ -	$ -	$ -
35	Acc-43	$ -	$ -	$ -	$ -
36	Acc-44	$ 96,250	$ 368,959	$ 185,959	$ 651,167
37	Acc-45	$ 914,805	$ 378,237	$ 160,112	$ 1,453,155
38	Acc-46	$ 791,169	$ 214,157	$ 98,598	$ 1,103,924
39	Acc-47	$ 129,736	$ (15,909)	$ -	$ 113,828
40	Acc-48	$ 574,075	$ 1,182,686	$ 745,545	$ 2,502,306
41	Acc-49	$ 343,289	$ (42,096)	$ -	$ 301,193
42	Acc-50	$ -	$ -	$ -	$ -
43	Acc-51	$ -	$ -	$ -	$ -

WhatsApp, et al. v. NSO Group, et al.
Presented Pegasus "Final Relevant Revenue" Excluding Time and Maintenance Adjustments (Q2 2018 - Q2 2020)
Supplemental Exhibit 1.1

	Account No.	Q2 - Q4 2018	2019	Q1 - Q2 2020	Q2 2018 - Q2 2020
44	Acc-53	$ -	$ -	$ -	$ -
45	Acc-54	$ -	$ -	$ -	$ -
46	Acc-55	$ -	$ -	$ -	$ -
47	Acc-56	$ -	$ 1,127,134	$ 159,667	$ 1,286,800
48	Acc-57	$ 855,852	$ 144,148	$ -	$ 1,000,000
49	Acc-61	$ -	$ -	$ -	$ -
50	Acc-62	$ -	$ -	$ -	$ -
51	Acc-63	$ -	$ -	$ -	$ -
52	Acc-66	$ 337,500	$ 448,695	$ 223,181	$ 1,009,376
53	Acc-67	$ -	$ -	$ -	$ -
54	Acc-68	$ 16,141	$ 21,541	$ 9,899	$ 47,580
55	Acc-69	$ -	$ -	$ -	$ -
56	Acc-70	$ -	$ -	$ -	$ -
57	Acc-71	$ 815,360	$ 224,314	$ 111,893	$ 1,151,566
58	Acc-72	$ 404,591	$ 109,874	$ 54,849	$ 569,315
59	Acc-73	$ 51,293	$ -	$ 27,420	$ 78,713
60	Acc-74	$ 890,211	$ -	$ -	$ 890,211
61	Acc-75	$ 529,697	$ 460,762	$ 78,789	$ 1,069,248
62	Acc-76	$ -	$ 981,264	$ 109,147	$ 1,090,411
63	Acc-77	$ -	$ -	$ 967,883	$ 967,883
64	Acc-78	$ -	$ -	$ -	$ -
65	Acc-79	$ -	$ 4,873,901	$ 1,794,195	$ 6,668,096
66	Acc-80	$ 1,357,418	$ -	$ -	$ 1,357,418
67	Acc-81	$ 58,333	$ 93,174	$ 69,808	$ 221,315
68	Acc-82	$ -	$ -	$ -	$ -
69	Acc-83	$ 131,250	$ 186,707	$ -	$ 317,957
70	Acc-84	$ -	$ -	$ -	$ -
71	Acc-85	$ -	$ 766,944	$ 97,741	$ 864,685
72	Acc-86	$ -	$ -	$ -	$ -
73	Acc-87	$ -	$ 2,400,000	$ 231,781	$ 2,631,781
74	Acc-88	$ -	$ -	$ -	$ -
75	Acc-89	$ -	$ -	$ -	$ -
76	Acc-90	$ 341,502	$ 54,640	$ -	$ 396,143
77	**Total**	**$ 19,439,947**	**$ 31,055,220**	**$ 11,213,759**	**$ 61,708,926**
78	**Accounts Generating Revenue**	**28**	**38**	**37**	**45**

Source: NSO_WHATSAPP_00045858. I have included revenue for accounts labeled "PGS" in "Product" column and "Yes" in "Covert Android was provided" column.
Calculated as revenue in columns C through K (revenue without considerations for time-based adjustments) multiplied by allocation presented for Covert Android deal portion (column V).