WILMER CUTLER PICKERING
HALE AND DORR LLP
BENJAMIN A. POWELL (SBN 214728)
Benjamin.Powell@wilmerhale.com
DAVID W. BOWKER (SBN 200516)
David.Bowker@wilmerhale.com
MOLLY M. JENNINGS (*pro hac vice forthcoming)*
Molly.Jennings@wilmerhale.com
1875 Pennsylvania Ave NW
Washington, DC 20006
Telephone: (202) 663-6000
Facsimile: (202) 663-6363

SONAL N. MEHTA (SBN 222086)
Sonal.Mehta@wilmerhale.com
2600 El Camino Real, Suite 400
Palo Alto, CA 94306
Telephone: (650) 600-5051
Facsimile: (650) 858-6100

Attorneys for Plaintiff Apple Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

APPLE INC.,

Plaintiff,

v.

NSO GROUP TECHNOLOGIES LIMITED, and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No. 5:21-cv-9078

COMPLAINT

DEMAND FOR JURY TRIAL

1. Plaintiff Apple Inc. ("Apple"), by and through its undersigned counsel, alleges the following against Defendants NSO Group Technologies Limited ("NSO") and Q Cyber Technologies Limited ("Q Cyber"):

INTRODUCTION

2. Defendants are notorious hackers—amoral 21st century mercenaries who have created highly sophisticated cyber-surveillance machinery that invites routine and flagrant abuse. They design, develop, sell, deliver, deploy, operate, and maintain offensive and destructive malware and spyware products and services that have been used to target, attack, and harm Apple users, Apple products, and Apple. For their own commercial gain, they enable their customers to abuse those products and services to target individuals including government officials, journalists, businesspeople, activists, academics, and even U.S. citizens.

3. These malicious activities have led the U.S. Government to impose sanctions against NSO. The U.S. Government confirms that Defendants' products and services "have … enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent. Such practices threaten the rules-based international order."[1]

4. Because of Apple's investment in, and longstanding commitment to, product security and privacy, there is critical need for the company's products around the world. There are 1.65 billion active Apple devices worldwide, consisting of over a billion iPhones and hundreds of millions of other active Apple devices such as Mac, iPad, and Apple Watch.

5. This action seeks redress for Defendants' multiple violations of federal and state law arising out of their egregious, deliberate, and concerted efforts in 2021 to target and attack Apple customers, Apple products and servers and Apple through dangerous malware and spyware that Defendants develop, distribute to third parties, and use (or assist others in using) to cause serious harm to Apple's users and Apple. Defendants did not breach data contained on Apple's

[1] U.S. Commerce Department, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://tinyurl.com/58s5zdpy.

servers, but did abuse Apple services and servers to perpetrate attacks on Apple's users and data stored on users' devices.

6. Apple has been a market leader in technology and innovation since the company's inception in 1976. From its groundbreaking personal computers—the Apple I, Apple II, and Macintosh, and iMac—to iPod, iPhone, iPad, Apple Watch, iCloud, and many other innovative hardware, software, and digital services, Apple has been at the revolutionary edge of the digital world for nearly half a century. As its product offerings have diversified over the years, Apple has remained committed to delivering the highest-quality devices and the most seamless user experiences. Apple has done so with a relentless focus on the needs and preferences of its customers.

7. Consistent with its focus on customers and its commitment to innovation, quality, and the user experience, Apple has prioritized and invested heavily in privacy protection and security features. Apple's best-in-class privacy and security features are the result of massive investment and years of effort to engineer and then consistently improve the company's operating systems, and industry-leading processes to identify vulnerabilities and rapidly deploy security patches that protect Apple customers. As a result, Apple is synonymous with security; indeed, iPhone has continuously defined the state-of-the-art in security protections.

8. Security researchers agree that iPhone is the safest, most secure consumer mobile device on the market. Over the past four years, Android devices were found to have 15 to 47 times more malware infections than iPhone. In addition, a recent study found that 98 percent of mobile malware targets Android devices.

9. The relative paucity of mobile malware targeting iOS users is not because Apple's customers are undesirable targets for hackers. Quite the opposite. It is Apple's dogged persistence to protect its customers that leads it to employ thousands of the world's very best engineers and experts, and spend billions of dollars annually, to create an ecosystem users can trust. In addition, Apple continuously and successfully fends off a variety of hacking attempts, malware payloads, and other cyberattacks. Apple has developed security features and regularly develops and deploys updates to protect its users from evolving threats and to prevent future attacks.

10. NSO is the antithesis of what Apple represents in terms of security and privacy. While Apple creates products to serve and protect its users, NSO targets and attempts to exploit those products to harm Apple and its users.

11. NSO's products are not ordinary consumer malware. NSO has no interest in serving up annoying pop-up ads or even spoofing your bank in order to siphon money from your checking account. NSO's products are far more insidious and often highly sophisticated. They permit attacks, including from sovereign governments that pay hundreds of millions of dollars to target and attack a tiny fraction of users with information of particular interest to NSO's customers. Average consumers are not of interest to or attacked by NSO or its customers.

12. NSO admits that its destructive products have led to violations of "fundamental human rights,"[2] which have been widely recognized and condemned by human rights groups and governments, including the U.S. Government.[3] To ensure that their products can be used by others to maximum effect, NSO reportedly provides ongoing technical support and other services to their clients as they deploy NSO's spyware against Apple's products and users, including journalists, human rights activists, dissidents, public officials, and others. Most recently, the Guardian reported that six Palestinian human rights defenders—one of whom is also a U.S. citizen—were attacked and surveilled using NSO's spyware.[4] Although NSO claims that its spyware "cannot be used to conduct cybersurveillance within the United States,"[5] U.S. citizens have been surveilled by NSO's spyware on *mobile* devices that can and do cross international borders.

13. NSO's malicious activities have exploited Apple's products, injured Apple's users, and damaged Apple's business and goodwill. NSO's malicious products and services have also required Apple to devote thousands of hours to investigate the attacks, identify the harm, diagnose the extent of the impact and exploitation, and develop and deploy the necessary repairs and patches

[2] NSO Transparency and Responsibility Report 2021 at 18, https://tinyurl.com/ffeu8k7e.

[3] U.S. Commerce Department, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://tinyurl.com/58s5zdpy.

[4] Stephanie Kirchgaessner & Michael Safi, *Palestinian activists' mobile phones hacked using NSO spyware, says report*, Guardian (Nov. 8, 2021), https://tinyurl.com/xue5c2vn.

[5] Response from NSO Group to the Pegasus Project, Wash. Post. (July 18, 2021), https://tinyurl.com/uwyukxfb.

to ensure that Apple servers, products, platforms, applications, and experiences remain safe and secure for more than a billion individuals and entities who comprise the global Apple community.

14. Defendants seek to operate with impunity by hiding behind their unnamed customers. Indeed, in response to another lawsuit brought against NSO and Q Cyber by other victims of their attacks, NSO and Q Cyber argued that they should enjoy some form of "sovereign immunity" based on the status of the governments to whom they claim they sell their products and services. But as the Ninth Circuit recently held, NSO and Q Cyber are not sovereigns and are not entitled to sovereign immunity. *See WhatsApp, Inc. v. NSO Group Technologies Ltd.*, No. 20-16408 (9th Cir. Nov. 8, 2021). Nor do they enjoy any other form of immunity for their unlawful commercial and tortious activity directed at Apple and its products, platforms, servers, and users in this country. Defendants' malicious and harmful activities have brought them well within the long arm of the law and the jurisdiction of this Court, which has the authority to hold them to account for their violations of U.S. federal and state laws and for the damage they have inflicted on Apple and its users.

THE PARTIES

15. Apple Inc. is a California corporation established in 1976, with its principal place of business in Cupertino, California. Apple designs, manufactures, and markets smartphones, personal computers, tablets, wearables, and accessories (e.g., iPhone, Mac, iPad, Apple Watch, and Apple TV), as well as related services (e.g., iCloud, the App Store, Apple Music, and Apple Pay).

16. Defendant NSO is an Israeli limited liability company incorporated on January 25, 2010, and, on information and belief, a subsidiary of Defendant Q Cyber. NSO designs highly invasive spyware, which it sells, distributes, operates, maintains, and services for third parties around the globe.

17. Defendant Q Cyber was incorporated in Israel on December 2, 2013, under the name L.E.G.D. Company Ltd. On May 29, 2016, L.E.G.D. Company Ltd. changed its name to Q Cyber. Until at least June 2019, NSO's website stated that NSO was "a Q Cyber Technologies company," and NSO stated as recently as July 2021 that NSO was a subsidiary of Q Cyber. Q

Cyber reportedly acts as a "commercial distributor" for NSO's products, including by signing contracts, issuing invoices, and receiving payments from NSO's customers.[6]

18. On information and belief, 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 were in the scope of that relationship. On information and belief, each Defendant knowingly and intentionally agreed with the other to carry out the acts alleged in this Complaint. On information and belief, in doing the acts and failing to act as alleged in this Complaint, each Defendant acted with the knowledge, permission, and consent of the other; and each Defendant aided and abetted the other.

JURISDICTION AND VENUE

19. The Court has jurisdiction over all causes of action alleged in this Complaint pursuant to 28 U.S.C. § 1332 because there is complete diversity between Apple and each of the named Defendants, and because the amount in controversy exceeds $75,000.

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

21. 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 facts as Apple's federal law claims.

22. The Court has personal jurisdiction over Defendants because, on information and belief, they created more than one hundred Apple IDs to carry out their attacks and also agreed to Apple's iCloud Terms and Conditions ("iCloud Terms"), including a mandatory and enforceable forum selection and exclusive jurisdiction clause that constitutes express consent to the jurisdiction of this Court.[7]

23. In particular, by registering for iCloud, Defendants agreed that "the relationship between you and Apple shall be governed by the laws of the State of California, excluding its

[6] Yannick Lambert, *Luxembourg-linked firm NSO used zero-click hacking, study claims*, Luxembourg Times (Sept. 14, 2021), https://tinyurl.com/nhkap9cp.

[7] The iCloud Terms provisions quoted throughout this Complaint are materially similar across all operative versions. For ease of reference, the Complaint cites only to the language in the September 20, 2021 version of the Terms (attached as Ex. 1).

conflicts of law provisions" and that "[y]ou … agree to submit to the personal and exclusive jurisdiction of the courts located within the county of Santa Clara, California, to resolve any dispute or claim arising from this Agreement." Ex. 1 at 19. Defendants' consent to personal jurisdiction encompasses this lawsuit, because Count Three arises from Defendants' breach of this agreement, and the Court may exercise pendent personal jurisdiction over the remaining counts, which arise from a common nucleus of operative fact.

24. The Court has personal jurisdiction over Defendants for the additional, independent reason that they purposefully directed and targeted their unlawful actions at California; used Apple products and services to target and cause harm to Apple at its principal place of business in California; created Apple ID and iCloud accounts using Apple servers located in California; misused Apple ID accounts to send abusive commands to Apple servers; misused Apple servers to deploy malware and attack Apple users; on information and belief, commandeered the Apple devices of Apple users to illicitly spy on them, steal their personal information, and otherwise harm them; impaired the value and functioning of Apple devices in the process; and otherwise specifically and purposefully directed their actions at the products, services, and proprietary technology of Apple, which is incorporated and has its principal place of business in California.

25. The Court has personal jurisdiction for the additional, independent reason that Defendants also purposefully availed themselves of California's benefits by agreeing to the iCloud Terms of Service (which contain a forum-selection and exclusive jurisdiction clause selecting California courts), targeting Apple and Apple products and services and users to accomplish Defendants' business objectives, and otherwise engaging in significant activities directed at California. On information and belief, NSO also sought and/or accepted funding from California investors, as evidenced by the fact that a San Francisco-based private equity firm acquired a controlling stake in NSO in March 2014. And, on information and belief, NSO's founders reacquired the company in February 2019 with Novalpina Capital, a London private equity firm. Since July 2021, Berkeley Research Group, a California-based consulting firm, has managed the

fund that currently owns a majority stake in NSO.[8] NSO has also partnered with WestBridge Technologies, Inc., a U.S.-based subsidiary of Q Cyber, to market Defendants' products or services to U.S. entities[9] including at least one California municipal police department.[10] Defendants' marketing efforts were reportedly unsuccessful.[11]

26. The Court also has personal jurisdiction over Defendants under the federal long-arm statute for all the reasons set forth above with respect to California, and because the claims in this Complaint also arise from Defendants' actions purposefully directed at the United States, including their unlawful targeting, trespassing, and use of Apple servers (and, on information and belief, other Apple devices or platforms) located in the United States, including in California.

27. Defendants likewise purposefully availed themselves of the United States's benefits by engaging in all the activities set forth above with respect to California and the significant additional activities directed at the United States. NSO deploys its malware and spyware primarily through servers hosted at data centers located in the United States and Europe.[12] NSO has hired and consulted with various U.S.-based firms to help market its products and services, expand its business, and improve its public relations in the United States.[13] Q Cyber has also hired a U.S.-based public relations firm to provide strategic and regulatory counsel.[14]

28. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b)(2), as the threatened and actual harm to Apple was purposefully directed toward, and occurred in, this District. In addition, by agreeing to the forum selection clause in the iCloud Terms, Defendants agreed that venue is proper in this Court.

---

[8] Stephanie Kirchgaessner, *Manager of fund that owns Israeli spyware firm not yet given access to sensitive info*, Guardian (Oct. 7, 2021), https://tinyurl.com/durx744a.

[9] Drew Harwell, *How Washington power brokers gained from NSO's spyware ambitions*, Wash. Post (July 19, 2021), https://tinyurl.com/yfwpbppv.

[10] William Turton, *Israel's NSO Group Linked to Hacking Tool Pitched To U.S. Police*, Yahoo! Finance (May 12, 2020), https://tinyurl.com/mrrkp6d9.

[11] *Id.*

[12] Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus* (2021), at 32, https://tinyurl.com/235zu2pu (attached as Ex. 2).

[13] Harwell, *supra* note 9.

[14] Aaron Schaffer, *Israeli spyware company accused of hacking activists hires lobby firm*, Al-Monitor (Jan. 10, 2020), https://tinyurl.com/5dn7jrmy.

INTRADISTRICT ASSIGNMENT

29. Pursuant to Civil L.R. 3-2(d), this case may be assigned to the San Jose division because Apple is located in Santa Clara County.

FACTS

A. Apple Provides Market-Leading Security To Its Users

30. When Apple developed iPhone, personal computers or "PCs" were the world's primary computing tools. Although Apple computers such as the Mac offered industry-leading security, many other PCs in the marketplace had insufficient security features and were riddled with computer "viruses" from malicious software or "malware." PC users often encountered serious reliability issues because downloading software or visiting a website resulted in their machines becoming infected with malware.

31. Apple designed iPhone with the knowledge and intention that it would be a highly personal device where users would access, send, receive, and store some of their most sensitive and personal information. Apple understood that a much larger and more diverse universe of users would own iPhones, which they would use in a manner far more personal than PCs ever were, keep with them wherever they went, and rely upon for professional, personal, and emergency use of all kinds. Apple knew that iPhone had to be highly reliable and protected from malware; it could not fall victim to the fate of PCs—it needed to be different.

32. Accordingly, Apple invested a massive amount in researching and developing industry-leading security protections that would make iPhone as secure as possible, with new features and technology that would ensure end-to-end security of its hardware, software, and wireless communications.

33. As just one recent example, Apple released a security feature called "BlastDoor." BlastDoor takes incoming messages and unpacks and processes their contents inside a secure and isolated environment, where malicious code hidden inside a message cannot interact with or harm an Apple device's operating system, or gain access to an Apple user's data. Even still, Defendants discovered ways to bypass BlastDoor's initial implementation. Apple has continued to refine the

technology, and to date Apple is unaware of successful circumventions of BlastDoor by Defendants on devices running iOS 15.

34. Apple has also designed and implemented a "secure boot" across its devices. This feature protects the lowest levels of software against tampering and allows only trusted operating system software from Apple to load at startup. Secure boot depends on a hardware root of trust; Apple's system software then builds a chain of trust that verifies that each step of the boot process is functioning properly before handing over control. This protects Apple systems from malware infection upon boot.

35. Another example is Apple's development of Secure Enclave, a dedicated secure subsystem that provides the foundation for the secure generation and storage of the keys necessary for encrypting data at rest. The Secure Enclave is isolated from the main processor of an Apple device in order to provide an extra layer of security and to keep sensitive user data secure even if another component of the phone were compromised. Such redundant security measures help protect users' files at rest by avoiding exposure of long-lived encryption keys.

36. Apple also provides multiple layers of protection to help ensure that the third-party apps that run on its operating systems are free of known malware and have not been tampered with. Additional protections carefully monitor and mediate the access of third-party applications, which may suffer from defects that Apple would not tolerate in its own products.

37. These hardware and software innovations are continuously reinforced and maintained by Apple's Security Engineering and Architecture ("SEAR") team, which works to protect Apple's products, platforms, and devices every day around the world. SEAR is constantly working to identify and patch vulnerabilities and address security problems.

38. Apple's sustained, multi-layered security approach has been incredibly effective: it is extremely rare for a consumer to encounter malware on iPhone. Other companies have tried without success to match Apple's level of security. Experts agree that iPhone and iOS are safer

and more secure than the competition. An estimated 98 percent of mobile malware targets Android devices, rather than iPhone.[15]

39. In light of Apple's formidable security features and defenses, all but a very few truly exceptional malware attacks on Apple devices are unsuccessful. These attacks have been very carefully designed and deliberately targeted by highly sophisticated parties with extraordinary resources and capabilities—typically nation-states and their agencies or instrumentalities, or, in some cases, those that do business with them. The Defendants associate themselves with these entities to enable their malicious hacking of iOS, Android, and other technologies.

B. NSO's Exploits Target and Attack Apple, Apple Devices, and Apple Users

40. Defendants develop and deploy highly invasive spyware known collectively as "Pegasus," which NSO describes as a "cyber intelligence solution that enables [clients] … to remotely and covertly extract valuable intelligence from virtually any mobile device."[16] While Defendants claim that their technology helps prevent crime, the U.S. Government's addition of NSO to the Entity List makes clear that laudable uses of this technology are not the only ones that NSO permits. Instead, on information and belief, Defendants conceal the enormous amounts of money they make from it and the despicable ways it is put to use.

41. According to Defendants and news reports, Pegasus is installed remotely on a device through fraud or deception and/or without its owner's awareness or consent. Defendants and their clients can then issue commands to Pegasus remotely to surveil an owners' activities and communications and to steal and transmit an owners' personal data from the infected device in a variety of insidious ways. Pegasus can record using a device's microphone and camera, track the phone's location data, and collect emails, text messages, browsing history, and a host of other information accessible through the device.[17]

---

[15] Apple, *Building a Trusted Ecosystem for Millions of Apps: A threat analysis of sideloading* (Oct. 2021), https://tinyurl.com/u3z69pav.

[16] *WhatsApp v. NSO Group, et. al*, No. 4:19-cv-7123 (N.D. Cal. Oct. 29, 2019), Dkt. 1-1 at 44.

[17] *WhatsApp v. NSO Group, et. al*, No. 4:19-cv-7123 (N.D. Cal. Oct. 29, 2019), Dkt. 1-1 at 40.

42. The Washington Post reported in July 2021 that Defendants and their clients have deployed Pegasus to attack and surveil scores of individuals, including journalists, human rights activists, government officials, and dissidents across more than 50 countries.[18] In the past year, for example, Amnesty International has said it discovered Pegasus spyware on the iPhones of a French human rights lawyer, a French human rights activist, an Indian journalist, and a Rwandan activist.[19]

43. Due to the severity and prevalence of the human rights abuses committed through NSO's spyware, the U.S. Government recently prohibited NSO from receiving U.S. exports of hardware or software. On November 4, 2021, the U.S. Commerce Department's Bureau of Industry and Security published a final rule adding NSO to its "Entity List" for engaging in activities contrary to the national security or foreign policy interests of the United States. As a result of this U.S. Government sanction, U.S. companies are now prohibited from exporting certain products and services to NSO without a special U.S. license (which the U.S. government will apply a presumption of denial for any such license applications by U.S. companies).[20] In an accompanying statement, the Commerce Department stated that this decision was "based on evidence that [NSO] developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers."[21]

44. According to reports by a Dublin-based human rights organization, the mobile phones of six Palestinian human rights defenders—including at least one U.S. citizen—were hacked using Pegasus.[22]

---

[18] Dana Priest, et al., *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, Wash. Post (July 18, 2021), https://tinyurl.com/h5pwd3uz.

[19] Ex. 2 at 32.

[20] U.S. Commerce Department, *Addition of Certain Entities to the Entity List*, 86 Fed. Reg. 60,759 (Nov. 4, 2021), https://tinyurl.com/8tpp38ve.

[21] U.S. Commerce Department, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://tinyurl.com/58s5zdpy.

[22] Stephanie Kirchgaessner & Michael Safi, *Palestinian activists' mobile phones hacked using NSO spyware, says report*, Guardian (Nov. 8, 2021), https://tinyurl.com/xue5c2vn.

45. In light of Apple's continually evolving security measures, delivering and installing Pegasus on an individual iPhone or any other Apple device is very difficult. As NSO itself has acknowledged, each "installation" of Pegasus on target devices must be "carefully planned to ensure it is successful."[23]

46. Upon information and belief, a core component of Defendants' design and deployment of Pegasus entails targeting Apple devices, studying Apple systems to discern new ways to attack Apple devices without the consent of Apple or its users, planning specific attacks on Apple devices and users, and working with clients to ensure that Defendants' spyware payload is delivered and operated to maximum effect. On information and belief, in furtherance of this effort, Defendants have used Apple devices, created Apple ID accounts, and agreed to the iCloud Terms.

47. As Defendants develop and deploy new exploits, SEAR must identify and investigate them, research and develop patches and solutions, and swiftly upgrade Apple hardware and software to prevent future similar attacks.

48. On information and belief, from at least February until September 2021, Defendants deployed their Pegasus spyware through an exploit that Citizen Lab named "FORCEDENTRY."[24] (Citizen Lab is a security-research organization based at the Munk School of Global Affairs & Public Policy, University of Toronto that investigates digital espionage against civil society.)[25]

49. Unlike exploits that require some action by the victim, such as clicking a hyperlink in a text message, FORCEDENTRY is known as a "zero-click" exploit, meaning that it allowed Defendants or their clients to hack into the victim's device without any action or awareness by the victim. FORCEDENTRY was first detected in March 2021, and subsequent forensic analysis by researchers at Citizen Lab and Amnesty International made a high-confidence attribution of the exploit to Defendants.

[23] *WhatsApp v. NSO Group, et. al*, No. 4:19-cv-7123 (N.D. Cal. Oct. 29, 2019), Dkt. 1-1 at 36.

[24] Bill Marczak, et al. *FORCED ENTRY: NSO Group iMessage Zero-Click Exploit Captured in the Wild*, Citizen Lab (Sept. 13, 2021), https://tinyurl.com/49j8wu56 (attached as Ex. 3).

[25] About the Citizen Lab, *Citizen Lab*, https://tinyurl.com/ykwp8ayx.

50. On information and belief, Defendants created more than one hundred Apple IDs using Apple's systems to be used in their deployment of FORCEDENTRY.

51. On information and belief, after obtaining Apple IDs, Defendants executed the FORCEDENTRY exploit first by using their computers to contact Apple servers in the United States and abroad to identify other Apple devices. Defendants contacted Apple servers using their Apple IDs to confirm that the target was using an Apple device. Defendants would then send abusive data created by Defendants through Apple servers in the United States and abroad for purposes of this attack. The abusive data was sent to the target phone through Apple's iMessage service, disabling logging on a targeted Apple device so that Defendants could surreptitiously deliver the Pegasus payload via a larger file. That larger file would be temporarily stored in an encrypted form unreadable to Apple on one of Apple's iCloud servers in the United States or abroad for delivery to the target.

52. According to cybersecurity research and news reports, following the delivery of Pegasus to an Apple device, Pegasus would begin transmitting personal data to a command-and-control server operated by Defendants or their clients. The operator, through the command-and-control server, was then able to issue commands to the device, including turning on the device's microphone or camera to record.[26] On information and belief, Defendants provide consulting and expert services to their clients, assist them with their deployment and use of Pegasus, and participate in their attacks on Apple devices, servers, and users.

53. Apple first received specific technical information about FORCEDENTRY from Citizen Lab on September 7, 2021. After extensive research, engineering, and testing around the clock over the next days, on September 13, 2021, Apple released iOS 14.8, along with updates for other Apple operating systems that included security updates to address the vulnerability.

54. Although Apple continues to consistently and efficiently secure its system against such exploits, Apple incurs substantial costs, redirects resources, and otherwise suffers harm and damages as a result of each attack. In the meantime, on information and belief, Defendants

[26] *NSO Group / Q Cyber Technologies: Over One Hundred New Abuse Cases*, Citizen Lab (Oct. 29, 2019), https://tinyurl.com/96dptdzm.

continue with their pernicious efforts to target, and harm Apple and its customers by infecting, exploiting, and misusing Apple devices and software.

55. Defendants' actions are apparently highly lucrative. NSO reportedly has revenue and earnings in the hundreds of millions of dollars from its spyware products and services. On information and belief, NSO has asked for fees in excess of one hundred million dollars for a single license and charges tens of millions of dollars per customer for its products and services. At times, the company reportedly has been valued at approximately one billion dollars.

C. NSO's Actions Have Injured Apple And Its Users

56. Defendants' injurious actions have included all of the misconduct described in the foregoing paragraphs, which are incorporated by reference herein, including but not limited to the development, deployment, maintenance, servicing, operation and other use of Pegasus and other spyware, malware and hacking devices to target, attack, exploit, and cause harm to Apple's goodwill, products and property, as well as Apple users' products and property.

57. These actions injured, harmed, and caused damages to Apple by forcing it to incur costs and to devote personnel, resources, and time to identifying and investigating the attacks and exploits; developing and deploying security patches and software upgrades; communicating with Apple personnel and users regarding such attacks, exploits, patches, and upgrades; increasing security measures to detect and prevent future attacks; and assessing and responding to legal exposure.

58. For example, and as discussed above, as soon as Apple discovered Defendants' malware attacks, SEAR worked quickly to obtain a sample of the FORCEDENTRY exploit and worked around the clock to investigate possible vulnerabilities, rapidly develop and deploy an update to protect Apple users, and continue to monitor Defendants' ongoing behavior. Apple's SEAR team has spent thousands of hours addressing Defendants' abusive actions.

59. Apple has been required to expend time and resources responding to government inquiries concerning the attacks.

60. Defendants force Apple to engage in a continual arms race: Even as Apple develops solutions and enhances the security of its devices, Defendants are constantly updating their malware and exploits to overcome Apple's own security upgrades.

61. These constant recovery and prevention efforts require significant resources and impose huge costs on Apple. Defendants' unlawful malware activities have caused and continue to cause Apple significant damages in excess of $75,000 and in an amount to be proven at trial.

CLAIMS FOR RELIEF

Count One

Violations of Computer Fraud and Abuse Act

18 U.S.C. § 1030(a)

62. Apple realleges and incorporates by reference all preceding paragraphs.

Access to Apple User Devices In Violation of 18 U.S.C. § 1030(a)(2), (a)(4)

63. Apple realleges and incorporates by reference all preceding paragraphs.

64. Apple's users' devices are "computers" as defined by 18 U.S.C. § 1030(e)(1).

65. Apple's users' devices are "protected computers" as defined by 18 U.S.C. § 1030(e)(2)(B) because they are "used in or affecting interstate commerce or communication."

66. Defendants violated and attempted to violate 18 U.S.C. § 1030(a)(2) because they intentionally accessed and attempted to access the iOS operating system on Apple's users' devices without authorization and, on information and belief, obtained information from Apple's users' devices.

67. Defendants violated 18 U.S.C. § 1030(a)(4) because they knowingly and with the intent to defraud accessed the operating system on Apple's users' devices without authorization using information from Apple's servers and then installed highly invasive spyware on those Apple users' devices, and by means of such conduct furthered the intended fraud and obtained something of value.

68. Defendants' access was without authorization because Apple's users never consented to Defendants accessing their devices to install their Pegasus spyware.

69. As a result of the fraud, Defendants obtained something of value, namely sensitive personal information, including text messages, emails, videos, images, and browser data, from Apple's users' devices.

70. Apple retains ownership of its operating-system software pursuant to its Software License Agreements.[27]

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

72. Defendants' actions caused Apple to incur a loss as defined by 18 U.S.C. § 1030(e)(11), in an amount in excess of $5,000 during a one-year period, including the expenditure of resources to investigate and remediate Defendants' conduct. Apple is entitled to compensatory damages in an amount to be proven at trial, as well as injunctive relief or other equitable relief. *See* 18 U.S.C. § 1030(g).

Damage to Apple User Devices In Violation Of 18 U.S.C. § 1030(a)(5)

73. Apple realleges and incorporates by reference all preceding paragraphs.

74. Defendants violated 18 U.S.C. § 1030(a)(5)(A) because they knowingly caused the transmission of a program, information, code, and/or command, specifically the commands needed to carry out the exploits described above, as well as the Pegasus spyware itself, to Apple's servers, and as a result of such conduct intentionally caused damage without authorization to the operating system on Apple's users' devices, including by installing their Pegasus spyware.

75. Defendants violated 18 U.S.C. § 1030(a)(5)(B) because they intentionally accessed Apple's users' devices without authorization and as a result of such conduct, recklessly caused damage to the operating system on Apple's users' devices, including by installing their Pegasus spyware.

76. Defendants violated 18 U.S.C. § 1030(a)(5)(C) because they intentionally accessed Apple's users' devices without authorization and as a result of such conduct, caused damage to the operating system on Apple's users' devices, including by installing their Pegasus spyware.

[27] *See* iOS and iPad OS Software License Agreement, https://tinyurl.com/4pwxdcc5.

77. Apple retains ownership of its operating-system software pursuant to its Software License Agreements.[28]

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

79. Defendants' actions caused Apple to incur a loss as defined by 18 U.S.C. § 1030(e)(11), in an amount in excess of $5,000 during a one-year period, including the expenditure of resources to investigate and remediate Defendants' conduct. Apple is entitled to compensatory damages in an amount to be proven at trial, as well as injunctive relief or other equitable relief. *See* 18 U.S.C. § 1030(g).

Count Two

Violations of California Business and Professions Code § 17200

80. Apple realleges and incorporates by reference all preceding paragraphs.

81. Defendants' actions described above constitute unlawful acts or practices in the conduct of business, in violation of California's Business and Professions Code Section 17200, *et seq.*, including actions that are forbidden by other laws.

82. Defendants' business practices are unlawful. As stated above, Defendants' conduct violated 18 U.S.C. § 1030.

83. As a result of Defendants' various acts and omissions, Apple was injured in fact and lost money and property in the form of, among other things, costs to investigate, remediate, and prevent Defendants' wrongdoings, in an amount to be proven at trial, and in excess of $75,000.

84. As a result of Defendants' unlawful acts, Apple has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

Count Three

Breach Of Contract

85. Apple realleges and incorporates by reference all preceding paragraphs.

[28] *See* iOS and iPad OS Software License Agreement, https://tinyurl.com/4pwxdcc5.

86. Since on or about August 2019, Defendants have created and used more than one hundred Apple IDs and, in doing so, agreed to the iCloud Terms.

87. The iCloud Terms constitute binding and enforceable contracts between Defendants and Apple.

88. Apple has performed all conditions, covenants, and promises required of it in accordance with the iCloud Terms.

89. Defendants' actions have breached the iCloud Terms, including at least the following provisions:

a. In Section V(B)(b), Defendants breached the agreement not to "use the Service to … stalk, harass, threaten or harm another";

b. In Section V(B)(h), Defendants breached the agreement "not to use the Service to … upload, post, email, transmit, store or otherwise make available any material that contains viruses or any other computer code, files or programs designed to harm, interfere or limit the normal operation of the Service (or any part thereof), or any other computer software or hardware";

c. In Section V(B)(i), Defendants breached the agreement not to "use the Service to … interfere with or disrupt the Service (including accessing the Service through any automated means, like scripts or web crawlers), or any servers or networks connected to the Service, or any policies, requirements or regulations of networks connected to the Service (including any unauthorized access to, use or monitoring of data or traffic thereon)";

d. In Section V(B)(j), Defendants breached the agreement not to "use the Service to … plan or engage in any illegal activity"; and

e. In Section V(B)(k), Defendants breached the agreement not to "use the Service to … gather and store personal information on any other users of the Service to be used in connection with any of the foregoing prohibited activities."

90. Defendants' many breaches have caused Apple to incur damages in an amount to be proven at trial, and in excess of $75,000.

91. Apple likewise seeks injunctive relief. As a direct result of Defendants' unlawful actions, Apple has suffered and continues to suffer irreparable harm for which there is no adequate remedy at law, and which will continue unless Defendants' actions are enjoined.

Count Four

Unjust Enrichment (In the Alternative to Count Three)

92. Apple realleges and incorporates by reference all preceding paragraphs.

93. Defendants' acts as alleged herein constitute unjust enrichment of the Defendants at Apple's expense.

94. Defendants received a benefit by profiting from the personal data they wrongfully obtained from Apple's users' devices through the improper use of Apple's servers, which is the central component of their lucrative Pegasus spyware sold to customers and deployed against journalists, activists, and dissidents around the globe. But for Defendants' conduct, they would not have obtained such profits.

95. Defendants' benefit came at Apple's expense because, as a result of Defendants' conduct, Apple was injured in fact and lost money and property in the form of, among other things, costs to investigate, remediate, and prevent Defendants' wrongdoing, and has suffered injury to its reputation, public trust, and goodwill as a market leader in offering best-in-class security features.

96. Defendants' retention of the personal data they wrongfully obtained from Apple's users' devices through the use of Apple's servers and the profits they derived therefrom would be unjust.

97. Apple seeks an accounting and disgorgement of Defendants' ill-gotten data and profits in an amount to be proven at trial, and in excess of $75,000.

PRAYER FOR RELIEF

WHEREFORE, Apple requests judgment against Defendants as follows:

A. A permanent injunction restraining Defendants from accessing and using any Apple servers, devices, hardware, software, applications, or other Apple products or services;

B. A permanent injunction requiring Defendants to identify the location of any and all information obtained from any Apple users' Apple devices, hardware, software, applications, or other Apple products—and to delete all such information, and to identify any and all entities with whom Defendants shared such information;

C. A permanent injunction restraining Defendants from developing, distributing, using, and/or causing or enabling others to use any spyware, malware or other malicious devices on Apple devices, hardware, software, applications, or other Apple products or services without Apple's (and, if applicable, the relevant Apple user's) consent;

D. Compensatory damages in an amount to be proven at trial;

E. Punitive damages;

F. An accounting of each Defendant's profits resulting from the conduct alleged above;

G. Disgorgement of Defendants' profits resulting from the conduct alleged above;

H. Any other such further relief as this Court deems just and proper.

Dated: November 23, 2021

Respectfully submitted,

By: */s/* Sonal N. Mehta

WILMER CUTLER PICKERING
HALE AND DORR LLP
BENJAMIN A. POWELL (SBN 214728)
Benjamin.Powell@wilmerhale.com
DAVID W. BOWKER (SBN 200516)
David.Bowker@wilmerhale.com
MOLLY M. JENNINGS
(*pro hac vice forthcoming*)
Molly.Jennings@wilmerhale.com
1875 Pennsylvania Ave NW
Washington, DC 20006
Telephone: (202) 663-6000
Facsimile: (202) 663-6363

SONAL N. MEHTA (SBN 222086)
Sonal.Mehta@wilmerhale.com
2600 El Camino Real, Suite 400
Palo Alto, CA 94306
Telephone: (650) 600-5051
Facsimile: (650) 858-6100

Attorneys for Plaintiff Apple Inc.