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 pending*)
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, California 94306
Telephone: (650) 600-5051
Facsimile: (650) 858-6100

Attorneys for Plaintiff Apple Inc.

Counsel for Defendants listed on signature page

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

APPLE INC.,

Plaintiff,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No. 3:21-cv-09078-JD

JOINT CASE MANAGEMENT STATEMENT

Hearing Date: February 17, 2022
Time: 10:00 am
Judge: Hon. James Donato

Pursuant to Civil Local Rule 16-9 and the Scheduling Order entered by the Court, Plaintiff Apple Inc. and Defendants NSO Group Technologies Limited and Q Cyber Technologies Limited (together, "Defendants"), respectfully submit this Joint Case Management Statement.

1. Jurisdiction and Service

Jurisdiction is contested, so the parties' respective positions are set forth immediately below. The parties agree that Defendants have waived service. Dkt. No. 17.

Plaintiff's Position: Plaintiff contends that this Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. §§ 1332 and 1331, as this action alleges violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a). This Court also has subject matter jurisdiction under 28 U.S.C. § 1367 over the state law claims presented in this action, namely, unlawful conduct of business, breach of contract, and unjust enrichment.

Plaintiff further contends that this Court has personal jurisdiction over both NSO Group and Q Cyber for several reasons. First, Defendants created Apple IDs to carry out their attacks and in doing so, agreed to the iCloud Terms and Conditions. Those Terms include a mandatory and enforceable forum selection and exclusive jurisdiction clause that constitutes express consent to the jurisdiction of this Court for claims arising out of the Terms. Defendants' consent to the iCloud Terms constitutes consent to this Court's jurisdiction over Apple's breach of contract claim. Apple's non-contract claims accordingly fall under the Court's pendent personal jurisdiction.

Second, and in any case, Defendants purposefully directed and targeted their unlawful actions at California by creating Apple IDs through Apple servers located in California; misused Apple servers to attack Apple users; and directing harm to Apple, which is incorporated and has its principal place of business in California. Defendants also availed themselves of California's benefits by agreeing to the iCloud Terms in connection with their attacks, thereby invoking the benefits and protections of this forum's laws. Each of these actions were specifically undertaken in relation to Defendants' underlying conduct at the center of Apple's claims.

Third, this Court has personal jurisdiction under the federal long-arm statute given all of the stated contacts with California, and because Defendants purposefully directed their unlawful conduct at Apple servers located in the United States, including in California. In addition,

Defendants have purposefully availed themselves of the United States' benefits by deploying malware through data centers located in the United States and engaging with U.S.-based firms.

This Court is also the proper venue for this action. Defendants purposefully directed harm toward this Judicial District when targeting Apple, and in any event, the forum-selection clause in the iCloud Terms, to which Defendants agreed, waives any objection to this venue.

Defendants' Position:

1. The Court lacks subject-matter jurisdiction because Defendants are immune under the common-law doctrine of conduct-based immunity. This argument was addressed by the Ninth Circuit in *WhatsApp Inc. v. NSO Group Technologies Ltd.*, 17 F.4th 930 (9th Cir. 2021), but the Ninth Circuit has stayed its mandate while Defendants file a petition to the U.S. Supreme Court for a writ of certiorari. On that basis, Defendants assert this argument here.

2. The Court lacks personal jurisdiction over Defendants.

First, Defendants did not consent to personal jurisdiction. Any ambiguity in the iCloud Terms must be resolved against Apple, and the iCloud Terms are ambiguous as to whether the forum-selection and jurisdiction clauses apply to foreign entities like Defendants. That ambiguity must be resolved in Defendants' favor, precluding a finding of consent.

Second, Apple has not identified any conduct by which Defendants purposefully targeted California or availed themselves of the benefit of California's laws. Apple argues that Defendants "direct[ed] harm to Apple," but there was no purposeful direction toward California as a state. *Axiom Foods, Inc. v. Acerchem Int'l, Inc.*, 874 F.3d 1064, 1068 (9th Cir. 2017). Apple's allegation that Defendants used Apple servers located in California does not show purposeful direction because the presence of any server in California would be fortuitous and due to Apple's own unilateral conduct. Apple does not and cannot allege that Defendants have any knowledge of or control over where Apple chooses to place its servers or which servers Apple data happens to pass through. And the law is clear that merely signing a contract such as the iCloud Terms is not purposeful availment of California's laws.

Third, there is no "federal long-arm statute" for any of Apple's claims. To the extent Apple means to reference Federal Rule 4(k)(2), Defendants do not have sufficient contacts with the

United States to support nationwide jurisdiction. Any use of U.S.-based servers was too fortuitous and attenuated to create jurisdiction under Rule 4(k)(2).

3. Venue is improper. Defendants neither consented to venue nor targeted this District. Apple's mere presence in the District does not support venue.

2. Facts

Plaintiff's Position: Defendants NSO Group and Q Cyber are notorious hackers, renowned for their creation, development, and deployment of highly sophisticated and destructive spyware technology. Plaintiffs assert that Defendants designed, developed, tested, deployed, marketed, sold, operated, maintained, and facilitated the use of their technology to maliciously target and harm Apple users, Apple products, and Apple itself. Defendants knowingly sold and facilitated the use of their malware and spyware to enable clients to attack a significant number of victims, including journalists, activists, dissidents, and even U.S. citizens. Defendants' misconduct has resulted in the U.S. Government blacklisting NSO Group, and instigated calls around the world for the imposition of additional sanctions and investigations into the pervasive misuse of Defendants' products to commit human rights abuses and other violations of law.

Apple's commitment to product security and privacy is at the core of its products and services—and one of the reasons why Apple's customers continue to invest in and rely upon Apple products and services. In light of Apple's formidable security features and defenses, it is very difficult to deploy Pegasus on any individual Apple device. Nonetheless, NSO has developed, tested, marketed, sold, deployed, used, and serviced Pegasus to enable targeting of Apple equipment and devices in order to surveil Apple users, including those of human rights activists and journalists. From at least February through September 2021, Defendants enabled and facilitated the deployment of their Pegasus spyware through an exploit that security researchers named "FORCEDENTRY." Unlike exploits that require some action by the victim for the victim's device to be compromised, FORCEDENTRY is known as a "zero-click" exploit, which means that Defendants or their clients have the ability to hack into the victim's device without any action—or awareness—by the victim.

Apple has reason to believe that Defendants created or facilitated the creation of more than

one hundred Apple IDs using Apple's systems and servers to deploy FORCEDENTRY. After obtaining these Apple IDs, Apple understands that Defendants executed or facilitated the execution of the FORCEDENTRY exploit first by using their computers to contact Apple servers in the United States and abroad to identify other Apple devices. After confirming that a target was using an Apple device, Defendants would then send abusive data through Apple servers in the United States and abroad using Apple's iMessage service. The abusive data would disable 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. Once Pegasus was installed, cybersecurity researchers report that Pegasus would begin transmitting personal data to a command-and-control server supplied by Defendants and operated by either Defendants or their clients. The operator was then able to issue commands to the device, including turning on the device's microphone or camera to record.

Defendants' exploitative activities have harmed Apple users and damaged Apple's goodwill, products, and property. Apple has devoted thousands of hours to investigate Defendants' attacks, diagnose the extent of the impact and exploitation, and develop and deploy the necessary repairs and patches to ensure that Apple servers, products, platforms, applications, and experiences remain safe and secure for the more than a billion individuals and entities who comprise the global Apple community.

Defendants' Position: Defendants are not hackers. NSO is an Israeli technology company that designs and markets a highly-regulated technology to government agencies for use in counterterrorism investigations and the investigations of child exploitation, cartel drug trafficking, and other serious crimes. Q Cyber, also an Israeli corporation, is NSO's sole director and majority shareholder. Defendants have no offices, employees, or other presence in California.

Defendants license their technology exclusively to government agencies for use in investigating and preventing terrorism and serious crime. Violent criminals and some of the world's most brutal and dangerous terrorists use Apple's services to plan and execute their crimes, while Apple disclaims responsibility and leaves it to others—governments and innocent victims—

to deal with the crimes Apple facilitates. NSO's technology allows government agencies to prevent crimes that Apple's technology would otherwise facilitate. The export of NSO's technology is regulated under Israel's Defense Export Control Law, and Defendants' customers are exclusively government agencies.

NSO's contracts with its customers require the customers to agree that they (1) will use NSO's technology "only for the prevention or investigation of crimes and terrorism and ensure that the [technology] will not be used for human rights violations" and (2) will immediately notify NSO of any misuse. Defendants contractually can suspend or terminate—and *have* suspended and terminated—service to customers engaged in improper use of NSO's technology outside these parameters. Moreover, Israel may deny or revoke export licenses if the Israeli government learns of an abuse of the technology or non-compliance with the intended use, such as a use of the technology to violate human rights.

Plaintiffs' allegations about Defendants' conduct are false. Most importantly, Defendants do not operate, and have never operated, their technology to surveil devices of third parties. Instead, the technology is operated exclusively by Defendants' government customers, with NSO acting in a purely tech-support capacity at its customers' direction. Defendants do not collect, store, or have any access to any information collected by its customers using NSO's technology. Defendants thus did not target any Apple device user, and in fact prohibit their customers from using NSO's technology against people who are not suspected terrorists or criminals. If a government ever misused NSO's technology to investigate Apple users other than criminals or terrorists, Defendants had no knowledge of that misuse, and it would have been a violation of that government's contract with NSO.

If anyone installed technology on any third-party Apple user's devices, therefore, it was not Defendants. And notably, Apple does not claim that Defendants or its customers unlawfully accessed any computer owned by Apple. Apple claims ownership only over its operating system, which is software, not a computer.

3. Legal Issues

1. Whether Defendants violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a);

2. Whether Defendants violated California's Business and Professions Code § 17200;
3. Whether Defendants breached the iCloud Terms;
4. Whether Defendants' alleged conduct constitutes unjust enrichment of Defendants at Apple's expense;
5. Whether Defendants are immune under common-law conduct-based immunity;
6. Whether Defendants' government customers are required parties under Rule 19;
7. Whether the Court has personal jurisdiction over Defendants;
8. Whether venue is proper in this District; and
9. Whether Apple can assert unjust enrichment as a separate cause of action or seek equitable relief.

4. Motions

Apple's motion for admission of Molly Jennings *pro hac vice* is pending. Dkt. 6.

Defendants will file a motion to dismiss on March 3, 2022. The parties are discussing a briefing schedule for that motion and, if they agree, will submit a proposed schedule to the Court.

If necessary, Defendants anticipate filing a motion to stay discovery pending their petition for certiorari in the *WhatsApp* litigation. If the parties cannot agree to a stipulated protective order, Defendants will move for the entry of a protective order.

The parties also anticipate that there will be further motions, including dispositive motions, motions to exclude expert testimony, and motions in limine. The parties reserve the right to file other motions not identified in this section.

5. Amendment of Pleadings

Apple has not amended the complaint under Federal Rule of Civil Procedure 15(a)(1)(A). Apple reserves the right to amend its complaint following Defendants' response to the complaint, *see* Fed. R. Civ. P. 15(a)(1)(B), and to seek leave to amend the complaint as needed.

6. Evidence Preservation

The parties each separately certify that they have reviewed the Guidelines Relating to the Discovery of Electronically Stored Information. The parties met and conferred as required by Federal Rule of Civil Procedure 26(f) on January 31, 2022, and addressed in detail the

requirements to preserve relevant evidence during that discussion.

7. Disclosures

Plaintiff's Position: Defendants advised Apple of their objection to the initial disclosures requirement the afternoon before this statement was due. In an attempt to address that objection, Apple has proposed that the parties agree to a short extension of the initial disclosures deadline and that the parties exchange initial disclosures on an "outside counsel's eyes only" basis if that deadline falls before the Court has entered a protective order in this case. The parties will submit any agreement affecting the initial disclosures deadline to the Court pursuant to L.R. 6-1(a).

Defendants' Position: The parties did not discuss initial disclosures during the Rule 26(f) conference because Apple dominated the available time with excessive questioning about Defendants' document preservation policies. Defendants offered to conduct a follow-up conference to discuss issues that were not discussed during the initial conference, and Apple declined, taking the position that any additional issues could be addressed in the exchange of drafts of this statement. That is what Defendants did. Defendants cannot exchange initial disclosures until the Court has issued a protective order. Defendants object to making initial disclosures before the Supreme Court resolves Defendants' petition for certiorari in the *WhatsApp* litigation and this Court resolves the jurisdictional and venue issues Defendants will raise in their motion to dismiss.

8. Discovery

The parties have not propounded any discovery. The parties have discussed the need for a protective order and intend to make a joint stipulation for the Court's consideration. The parties also plan to negotiate and submit a stipulated e-discovery order for the Court's consideration.

Plaintiff's Position: Apple intends to seek documents and testimony from the Defendants regarding, among other things: Defendants' development, testing, marketing, and selling of the FORCEDENTRY exploit and/or Pegasus and other exploits or products targeting Apple servers, equipment, and devices; Defendants' deployment of the FORCEDENTRY exploit and/or Pegasus, and any other exploits or products, against Apple servers, equipment, and devices and/or Apple users; Defendants' interactions with their clients in connection with the deployment of FORCEDENTRY and/or Pegasus, and any other exploits or products, against Apple servers,

equipment, and devices and/or Apple users; the identities of Defendants' clients and victims; representations Defendants made concerning FORCEDENTRY and/or Pegasus and/or other exploits or products; the relationship between NSO Group and Q Cyber; revenue and profits earned from Pegasus and/or other exploits or products; NSO's reported purchase of critical components from the United States; NSO's contacts with U.S.-based clients and potential clients; and financing NSO has received from U.S.-based entities.

Defendants' Position: Defendants do not believe that discovery is appropriate until the Supreme Court resolves their petition for certiorari in the *WhatsApp* litigation and this Court resolves the jurisdictional issues in Defendants' motion to dismiss. In any event, the discovery Apple claims to seek is overbroad and unreasonable and includes information that is not relevant to Apple's allegations, information that is not within Defendants' custody or control, and/or information that Defendants are prohibited from disclosing under applicable law. Until the parties agree to a protective order and Apple serves actual, targeted discovery requests, Defendants cannot determine whether they will be able or willing to produce the information Apple describes.

9. Class Action

This case is not a class action.

10. Related Cases

The parties are not aware of any cases that satisfy the standard for relation in L.R. 3-12(a). The parties do, however, wish to bring to the Court's attention *WhatsApp LLC et al. v, NSO Group Technologies Limited, et al.*, No. 4:19-cv-7123-PJH (N.D. Cal.), which involves some legal and factual issues that overlap with this case.

11. Relief

Plaintiff's Position: Apple is seeking compensatory damages based on the thousands of hours its engineers spent investigating the attacks, remediating them, and notifying affected users. The formula for calculating those damages will include, at a minimum, the total number of hours spent and the value of those hours, which will be based on, *inter alia*, the fully-loaded salary expenses for the relevant individuals and the time spent by each individual. There is no question that the product of this damages formula will exceed the $75,000 minimum for diversity

jurisdiction. Apple may rely on expert testimony to calculate the fully-loaded value of those hours. Apple's damages will also include hard costs associated with the investigation. Apple is in the process of estimating these damages and will provide further detail on its damages computation and supporting evidence in its Initial Disclosures, which it intends to serve on February 14 or a date thereafter as agreed by the parties. Apple is also seeking punitive damages, an accounting of each Defendant's profits, and disgorgement of the profits associated with Defendants' illegal attacks on Apple, the amount of each will be informed by discovery and potentially also expert testimony. Apple has suffered additional harms as described in the Complaint and also seeks injunctive relief.

Defendants' Position: Plaintiffs' statement of the relief sought is inadequate because it does not identify "the amount of any damages sought"—as the Court's Standing Order requires—other than the bare statement that it exceeds $75,000. Defendants contend that Apple is not entitled to most of the damages described in its statement. Apple is also not entitled to the equitable remedy of disgorgement because it seeks an adequate legal remedy. Apple's requested injunction seeks relief that only Defendants' government customers can provide, making those customers required parties under Rule 19.

12. Settlement and ADR

No settlement discussions have taken place. The parties discussed ADR during the Rule 26(f) conference and elected to discuss options during the Case Management Conference.

13. Consent to Magistrate Judge For All Purposes

The parties do not consent to proceed before a magistrate judge for all purposes.

14. Other References

This case is not suitable for reference to arbitration, a special master, or the JPML.

15. Narrowing of Issues

The parties do not believe that any issues can be narrowed by agreement at this time.

16. Expedited Trial Schedule

The parties agree that this case is not amenable to the Expedited Trial Procedure.

17. Scheduling

Plaintiff's position: Apple respectfully proposes the following pretrial schedule:

Event	Deadline
Fact discovery cut-off	December 9, 2022
Expert Disclosures	January 18, 2023
Responses to Expert Disclosures	February 17, 2023
Expert discovery cut-off	March 10, 2023
Last day to file dispositive and *Daubert* motions	April 10, 2023
Summary judgment opposition due	May 10, 2023
Summary judgment replies due	June 9, 2023
Pretrial conference	July 13, 2023
Jury Trial	August 7, 2023

Defendants' Position: Defendants believe the Court should hold a further conference to set the pretrial schedule only if and after the Court determines that is has subject-matter and personal jurisdiction and that venue is appropriate in this District. If the Court wishes to set a pretrial schedule at the initial case-management conference, Defendants do not believe discovery can reasonably be completed before December 2023 due to the potential for an extended motion-briefing schedule, the multi-jurisdictional nature of the discovery in this case, and the need for the involvement of multiple third parties. After the Court enters a protective order, Defendants will be able to describe in more detail the basis for its position. Otherwise, Defendants believe the spacing of deadlines proposed by Apple to be generally reasonable.

18. Trial

Apple requests a jury trial and estimates that the trial in this case will take two weeks.

19. Disclosure of Non-Party Interested Entities or Persons

Apple filed its disclosures November 23, 2021. Counsel for Apple recertifies that Apple Inc. has no parent corporation, that no publicly held corporation holds 10% or more of Apple's stock, and that Apple is not aware of any reportable persons or entities under Local Rule 3-15.

Defendants have filed their disclosures. They recertify that Q Cyber is NSO's parent corporation, and OSY Technologies is Q Cyber's parent corporation. Defendants are not aware of any other reportable persons or entities under L.R. 3-15.

20. Professional Conduct

All attorneys of record have reviewed the District's Guidelines for Professional Conduct.

Dated: February 10, 2022

WILMER CUTLER PICKERING HALE AND DORR LLP

By: /s/ David W. Bowker
DAVID W. BOWKER

Attorneys for Plaintiff
APPLE INC.

Dated: February 10, 2022

KING & SPALDING LLP

By: /s/ Joseph N. Akrotirianakis
JOSEPH N. AKROTIRIANAKIS

Attorneys for Defendants
NSO GROUP TECHS. LTD. and Q CYBER TECHS. LTD.

SIGNATURE ATTESTATION

I am the ECF User whose identification and password are being used to file the foregoing. Pursuant to Civil Local Rule 5-1(i), I hereby attest that the other signatories have concurred in this filing.

Dated: February 10, 2022

By: */s/* David W. Bowker
David W. Bowker