

1 JOSEPH N. AKROTIRIANAKIS (Bar No. 197971)
jakro@kslaw.com
2 AARON S. CRAIG (Bar No. 204741)
acraig@kslaw.com
3 KING & SPALDING LLP
633 West Fifth Street, Suite 1600
4 Los Angeles, CA 90071
Telephone: (213) 443-4355
5 Facsimile: (213) 443-4310

6 Attorneys for Defendants NSO GROUP TECHNOLOGIES
LIMITED and Q CYBER TECHNOLOGIES LIMITED
7

8 UNITED STATES DISTRICT COURT
9 NORTHERN DISTRICT OF CALIFORNIA
10 OAKLAND DIVISION

11
12 WHATSAPP INC., a Delaware corporation,
and FACEBOOK, INC., a Delaware
13 corporation,

14 Plaintiffs,

15 v.

16 NSO GROUP TECHNOLOGIES LIMITED
and Q CYBER TECHNOLOGIES LIMITED,

17 Defendants.
18
19

Case No. 4:19-cv-07123-PJH

**DEFENDANTS NSO GROUP
TECHNOLOGIES LIMITED
AND Q CYBER TECHNOLOGIES
LIMITED'S RESPONSE TO
PLAINTIFFS' BRIEF ON DISCOVERY
FROM CITIZEN LAB**

Ctrm: 3
Judge: Hon. Phyllis J. Hamilton

Action Filed: 10/29/2019


**[REDACTED VERSION OF
DOCUMENT SOUGHT TO BE SEALED]**


20
21
22
23
24
25
26
27
28

1 **I. INTRODUCTION**

2 The Court ordered Plaintiffs to “state [their] intentions with respect to the ‘civil-society’-
3 related allegations” that permeate the Complaint and other filings (Dkt. 299 at 3). Plaintiffs instead
4 used most of their five pages as an pseudo-motion in limine to exclude certain arguments at trial.
5 That is inappropriate—this is a discovery motion, devoted to deciding whether the evidence NSO
6 seeks is *relevant* to Plaintiffs’ claims or NSO’s defenses, not to deciding which claims or defenses
7 can be presented at trial. In any event, Plaintiffs’ brief acknowledges that they will seek to
8 introduce the “civil society” evidence at trial. The Letter Rogatory should thus issue.

9 The evidence Defendants seek from Citizen Lab is plainly relevant. Plaintiffs’ brief makes
10 clear that they intend to argue at trial that NSO is a bad-faith hacker that “sen[t] malicious code
11 through Plaintiffs’ servers to the Target Users.” (Dkt. 300 at 2.) That is not true—NSO designed
12 a law-enforcement technology, materially no different from a wiretap, that governments (and only
13 governments, and never NSO itself or any private entity) use in lawfully authorized intelligence
14 and law-enforcement investigations. NSO obviously will need to explain to the jury what Pegasus
15 is; otherwise the jury will have no understanding of why Pegasus was developed and how it is
16 actually used, and it may wrongly infer, for example, that NSO designed and uses Pegasus to
17 access users’ credit cards and bank accounts. Pegasus’s actual law-enforcement and counter-
18 terrorism purposes are relevant to, among other things, whether NSO can be liable for any of the
19 conduct Plaintiffs challenge, whether any of the alleged access to Plaintiffs’ servers was
20 “authorized” under the CFAA, and, as Plaintiffs themselves point out, whether they are entitled to
21 their requested remedies. Because Plaintiffs admit they intend to respond to NSO’s evidence with
22 Citizen Lab’s analysis alleging that some governments have used NSO’s technology to monitor
23 members of “civil society” (which would be beyond the scope of any license granted by NSO and
24 the Government of Israel), NSO is entitled to discovery from Citizen Lab about that analysis.

25 The evidence Plaintiffs themselves have produced about Citizen Lab’s investigation is
26 incomplete and inadequate. It consists of a conclusory spreadsheet 

27 
28 Neither the spreadsheet, nor anything else Plaintiffs have produced, explains *how* Citizen Lab

1 conducted its analysis or came to its conclusions, and Citizen Lab itself [REDACTED]
2 [REDACTED] Plaintiffs cannot deny NSO discovery
3 into this information by outsourcing the analysis to a foreign entity outside of the subpoena power.

4 **II. NSO IS ENTITLED TO EXPLAIN ITS BUSINESS AND TECHNOLOGY AT TRIAL**

5 Even though Plaintiffs based their complaint, and almost every filing they have submitted
6 in this case, around a false claim that NSO uses its technology to target members of “civil society”
7 like journalists and human rights activists (Dkt. 299 at 2), they now accuse *NSO* of “focus[ing] on
8 the identities of the Target Users throughout the litigation” and ask the Court to preclude NSO
9 from arguing that it designed and licenses its technology for law-enforcement purposes (Dkt. 300
10 at 3). That attempt to exclude NSO’s arguments and defenses has no place in the context of a
11 discovery motion. But even if it did, Plaintiffs’ arguments lack merit.

12 Although Plaintiffs’ brief leaves much about their intentions unclear, at least one thing is
13 plain: They will argue at trial that NSO designed and uses its technology for “malicious” purposes,
14 portraying NSO as nothing more than a common hacker. (*Id.*) NSO must be allowed to counter
15 that false narrative with the truth. To do so, NSO should be allowed to introduce *res gestae*
16 evidence that explains to the jury Pegasus’s *real* purpose: to enable sovereign governments that
17 have not built their own technology to conduct the same sort of intelligence-gathering, law-
18 enforcement, counterterrorism investigations routinely conducted in the United States by our own
19 government. Without that context, the jury will have no way of understanding what the case is
20 about, who NSO is, what its technology does, or why Pegasus exists.

21 Plaintiffs, of course, would prefer this case to be a one-sided “show” trial, in which
22 Plaintiffs get to smear NSO and prevent NSO from explaining the important purposes for which
23 its technology is licensed and used. Plaintiffs also want to hide from the jury relevant information
24 favorable to NSO, such as the fact—which Plaintiffs have no evidence to contradict—that NSO
25 only licenses its technology to governments and never operates the technology itself.
26 Simultaneously, Plaintiffs hope to hide relevant but negative information about Plaintiffs’ own
27 conduct, such as the fact that Plaintiffs’ obstruction of law-enforcement investigations make
28 technology like NSO’s necessary, or that Facebook tried to license Pegasus to spy on Apple users

1 but was refused *because* NSO does not license Pegasus to private companies. (Dkt. 45-11 ¶ 10.)

2 NSO has a right to dispute Plaintiffs' accusations and explain its alleged conduct to the
3 jury. In addition, evidence that NSO (regulated by Israel's strict export control and licensing
4 regime) designed and licenses its technology solely for intelligence-gathering, law-enforcement,
5 and counterterrorism investigations authorized by its customers' laws is relevant for several other
6 purposes. First, how Pegasus is used is relevant to whether any access to Plaintiffs' servers or
7 Target Devices was "authorized" under the CFAA. If a use of Pegasus was "lawfully authorized"
8 by a foreign government acting consistent with that nation's laws, then any access pursuant to that
9 legal authorization would not be "without authorization" or "exceed[] authorized access." *See* 18
10 U.S.C. § 1030(a), (f).¹ Second, as Plaintiffs concede, evidence that Pegasus is used for law-
11 enforcement purposes is relevant to whether NSO breached Plaintiffs' terms of service by
12 engaging in, for example, "illegal," or "impermissible" conduct. (Dkt. 1 ¶ 21; Dkt. 300 at 2 n.1.)
13 A lawful government investigation is not "illegal" or "impermissible." Third, who uses Pegasus
14 is relevant to whether NSO can be held liable for its clients' conduct. Because NSO licenses its
15 technology solely to be used in lawful intelligence and law-enforcement investigations, has no
16 operational role in any use of its technology, and shuts down improper uses of its technology, NSO
17 cannot be considered a co-conspirator with respect to any alleged abuse of its technology by a
18 foreign government. Nor, contrary to Plaintiffs' bizarre insinuation (Dkt. 300 at 3), can NSO be
19 secondarily liable under the CFAA for government conduct that does not itself violate the CFAA.²

20 Plaintiffs concede that they will respond to NSO's explanation about how Pegasus is used
21 by introducing Citizen Lab's "civil society" analysis. (*Id.* at 3-4.) That alone entitles NSO to
22

23
24 ¹ Plaintiffs point out that the CFAA's law-enforcement provision, § 1030(f), does not mention
25 foreign governments, but the fact that Pegasus is exclusively used by foreign governments still
26 bears on the meaning of "authorization" in § 1030(a). Otherwise, Plaintiffs' position would mean
that the CFAA prohibits foreign governments from conducting legally authorized searches of their
own residents' computers consistent with their own laws. That would be absurd.

27 ² Plaintiff's account of *United States v. Christensen*, 828 F.3d 763 (9th Cir. 2015), is dishonest.
28 The portion they cite had nothing to do with CFAA or CDAFA. *See id.* at 794 (discussing elements
specific to 18 U.S.C. §§ 2511(1)(a), 2512(1)(b)). *Christensen* in fact *reversed* the defendant's
CFAA conviction, *id.* at 786-87, and did not address CDAFA at all.

1 discovery into that analysis. Moreover, Plaintiffs’ brief is remarkably opaque about what they will
2 do with Citizen Lab’s analysis even if NSO does *not* introduce evidence about the uses of its
3 technology. Even though their pretrial disclosures stated an intent to call Citizen Lab witnesses
4 not just on the “civil society” allegations but also on “the identification of Defendants as
5 responsible for unauthorized access and abuse of the WhatsApp services” (Dkt. 293-3, Exh. B),
6 Plaintiffs now say they “do not *currently* intend to call any witness from Citizen Lab at trial.” But
7 that artfully phrased answer of course leaves open the possibility that Plaintiffs will change their
8 minds. (*Id.* at 2 (emphasis added).) And when Plaintiffs say they will not “use any of Citizen
9 Lab’s documents *that [they] have not already produced,*” this means they *do intend to use* Citizen
10 Lab documents that they *have* produced. (*Id.* (emphasis added).) If Plaintiffs intend to rely at all
11 on Citizen Lab’s analysis, then NSO is entitled to discovery into how Citizen Lab conducted that
12 analysis in order to attack the reliance the jury should place on it.

13 Finally, Plaintiffs argue their “civil society” allegations are relevant to their requests for
14 injunctive relief, disgorgement, and punitive damages. (*Id.* at 4.) That admission refutes Plaintiffs’
15 claim that evidence about the uses of Pegasus is irrelevant, and NSO is entitled to discovery into
16 the evidence Plaintiffs intend to use to support their requested remedies. Plaintiffs cannot seek
17 injunctive relief, disgorgement, or punitive damages by claiming that NSO’s technology “target[s]
18 journalists, human rights, activists, and opposition politicians” (*id.*) while simultaneously
19 preventing NSO from introducing evidence that, in fact, its technology is used to prevent and
20 punish crimes—particularly where *Plaintiffs’ own technology* facilitates and shields those crimes
21 from other means of investigation. Defendants should also be allowed to prove that uses of
22 Pegasus against true “civil society” would be unauthorized, *de minimis*, and dealt with harshly.

23 **III. EVIDENCE FROM CITIZEN LAB IS RELEVANT AND PROPORTIONATE**

24 Plaintiffs end their brief by arguing that the Court should deny NSO discovery from Citizen
25 Lab because, they argue, that discovery is not proportionate to the needs of the case. But, as NSO
26 has previously explained (and Plaintiffs have not disputed), Plaintiffs lack standing to oppose
27 discovery from a third party on that basis. (Dkt. 298 at 2); *e.g.*, *Doe v. Kaiser Found. Health Plan,*
28 *Inc.*, 2023 WL 8714880, at *3 (N.D. Cal. Dec. 17, 2023). Besides, if this Court issues a letter

1 rogatory, a Canadian court will independently apply Canadian law regarding proportionality and
2 other discovery limitations. This Court need not and should not prejudice those issues.

3 Anyway, it is badly disingenuous for Plaintiffs to claim they have already produced
4 sufficient information on Citizen Lab’s “civil society” analysis. Citizen Lab purports to have
5 identified up to [REDACTED] as being members of “civil
6 society.” Plaintiffs’ production reveals almost nothing about the methods used to arrive at this list
7 of “civil society” Target Users.³ On its face, however, the list itself indicates that even Citizen
8 Lab [REDACTED] members
9 of “civil society.” See Declaration of Aaron Craig (“Craig Decl.”) Exh. 1 and ¶¶ 2-7. Plaintiffs
10 have not produced any documents explaining Citizen Lab’s methods or why its [REDACTED]

11 [REDACTED] Because Plaintiffs have not produced such
12 documents, it can be presumed that they are solely in Citizen Lab’s possession. If Plaintiffs intend
13 to use their “civil society” allegations against NSO in this case, as their brief indicates, NSO must
14 be afforded adequate discovery into the reliability of those allegations. Plaintiffs should not be
15 permitted to shroud the process in secrecy by farming it out to a foreign entity beyond the subpoena
16 power of U.S. courts. Thus, the requested letter rogatory is necessary and proper.

17 **IV. CONCLUSION**

18 The Court should grant NSO’s motion for a letter rogatory.

19 DATED: April 12, 2024

KING & SPALDING LLP

20 By: /s/ Joseph N. Akrotirianakis

21 JOSEPH N. AKROTIRIANAKIS

AARON S. CRAIG

22 Attorneys for Defendants NSO GROUP

23 TECHNOLOGIES LIMITED and Q

24 CYBER TECHNOLOGIES LIMITED

25 ³ In an August 7, 2019 email, Citizen Lab’s John Scott-Railton says that Citizen Lab [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED] Craig Decl. Exh. 2.