

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

United States District Court
Northern District of California

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

WHATSAPP INC., et al.,
Plaintiffs,
v.
NSO GROUP TECHNOLOGIES
LIMITED, et al.,
Defendants.

Case No. 19-cv-07123-PJH

**ORDER RE MOTIONS TO COMPEL
AND MOTION FOR RELIEF FROM
CASE MANAGEMENT ORDER**

Re: Dkt. No. 235, 236, 239, 240, 249,
257, 260, 264, 265, 272, 276, 279, 280

Before the court are plaintiffs' motion to compel discovery, defendants' motion to compel discovery, and defendants' motion for relief from the case management schedule. The motions came on for hearing on February 15, 2024. Plaintiffs WhatsApp Inc. and Facebook, Inc. appeared through their counsel, Antonio Perez-Marques, Craig Cagney, Micah Block, and Greg Andres. Defendants appeared through their counsel, Joseph Akrotirianakis and Aaron Craig. Having read the parties' papers and carefully considered their arguments and the relevant legal authority, and good cause appearing, the court rules as follows.

BACKGROUND

On October 29, 2019, plaintiffs filed this lawsuit, alleging that defendants sent spyware, using WhatsApp's system, to approximately 1,400 mobile phones and devices designed to infect those devices for the purpose of surveilling the users of those phones and devices. Dkt. 1, ¶ 1. The complaint alleges four causes of action: (1) violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030; (2) violation of the California

1 Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502; (3)
2 breach of contract; and (4) trespass to chattels.¹

3 Defendants previously filed a motion for protective order, seeking an order
4 excusing it from compliance with discovery obligations due to various U.S. and Israeli
5 restrictions. See Dkt. 186. The court denied defendants' motion to the extent that it
6 sought a blanket order excusing it from all discovery, but also concluded that defendants
7 may be partially excused from certain discovery obligations based on the framework set
8 forth by Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir.
9 1992). See Dkt. 233.

10 The Richmark court set forth the following factors for a court to consider "in
11 deciding whether or not foreign statutes excuse non-compliance with discovery orders:"
12 (1) the importance to the investigation or litigation of the documents or other information
13 requested, (2) the degree of specificity of the request, (3) whether the information
14 originated in the United States, (4) the availability of alternative means of securing the
15 information, (5) and the extent to which noncompliance with the request would undermine
16 important interests of the United States, or compliance with the request would undermine
17 important interests of the state where the information is located. 959 F.2d at 1475.

18 After considering Richmark as applied to this case, the court concluded that "to the
19 extent that discovery disputes arise between the parties, the court's analysis will focus on
20 factors (1) and (2), and in instances where the requested discovery is sufficiently
21 important and specific, the court will order compliance with those discovery requests."
22 Dkt. 233 at 10.

23 Plaintiffs' motion to compel discovery now raises a dispute where the discovery
24 requests must be analyzed as to factor (1) and (2), i.e., the importance of the requests to
25 the litigation, and the degree of specificity of the requests.

26

27 _____
28 ¹ The court dismissed plaintiffs' fourth cause of action under Rule 12(b)(6), and no
amended complaint was filed. See Dkt. 111. That leaves only the first three causes of
action as operative claims in this case.

1 Defendants have also filed a motion to compel discovery that does not relate to
2 the Richmark factors, as well as a motion for relief from the case management schedule.
3 Those motions will be addressed after addressing plaintiffs' discovery motion. The
4 parties have also filed a number of motions to seal (Dkt. 235, 239, 249, 257, 260, 264,
5 272, 276), which are GRANTED.

6 DISCUSSION

7 A. Plaintiffs' motion to compel discovery (Dkt. 236)

8 As an initial matter, as stated at the hearing, defendants have already conceded
9 that some of plaintiffs' requests do seek information that is sufficiently important and
10 specific under Richmark, and those documents must indeed be produced. See Dkt. 252
11 at 5. As to the remaining discovery sought by plaintiffs' motion, the court will address
12 those requests with reference to the four categories set forth in the parties' briefs: (1)
13 what versions of the alleged spyware must be produced, (2) what functionality of the
14 alleged spyware must be produced, (3) whether defendants' clients must be disclosed,
15 and (4) whether defendants' server architecture information must be disclosed. See Dkt.
16 236 at 12.

17 As to category (1), as stated at the hearing, the court adopts plaintiffs' definition of
18 "all relevant spyware" as set forth in their motion: "any NSO spyware targeting or directed
19 at Whatsapp servers, or using Whatsapp in any way to access Target Devices." See Dkt.
20 236 at 13. As also stated at the hearing, defendants have not identified a basis for
21 limiting its production to the Pegasus program, or to any particular single operating
22 system. The complaint alleges that "Pegasus or another remote access trojan developed
23 by defendants" was responsible for the data breaches, and that the programs were used
24 "on mobile devices using the Android, iOS, and Blackberry operating systems." See Dkt.
25 1, ¶¶ 24, 32. Accordingly, the definition of "all relevant spyware" shall not be read to
26 include only Pegasus, or only a single operating system's program. Under Richmark,
27 those documents are sufficiently important and specific such that compliance with
28 discovery obligations may not be excused.

1 As to the timeframe of documents that must be produced, the court concludes
2 that, at this stage of the case, the Richmark factors weigh in favor of production for “all
3 relevant spyware” for a period of one year before the alleged attack to one year after the
4 alleged attack; in other words, from April 29, 2018 to May 10, 2020. See Dkt. 1, ¶ 42. If,
5 after reviewing the relevant spyware from that timeframe, plaintiffs are able to provide
6 evidence that any attack lasted beyond that timeframe, plaintiffs may seek further
7 discovery at that time. At the hearing, the parties discussed the possibility of stipulating
8 to a timeframe for the production of “all relevant spyware,” and may substitute their own
9 stipulation for the timeframe set forth in this order.

10 As to category (2), the court rejects defendants’ argument that their production
11 should be limited to the installation layer of the alleged spyware, and instead concludes
12 that defendants must produce information concerning the full functionality of the relevant
13 spyware. As discussed at the hearing, the complaint contains numerous instances
14 alleging not only that spyware was installed on users’ devices, but also that information
15 was accessed and/or extracted from those devices. See, e.g., Dkt. 1, ¶ 27 (“Pegasus
16 could ‘remotely and covertly extract valuable intelligence from virtually any mobile
17 device,’ . . . “intercept communications sent to and from a device, including
18 communications over iMessage, Skype, Telegram, WeChat, Facebook Messenger,
19 Whatsapp, and others,” and could be “customized for different purposes, including to
20 intercept communications, capture screenshots, and exfiltrate browser history.”); ¶ 32
21 (“Pegasus or another remote access trojan” was used “for the purpose of accessing data
22 and communications on target devices.”); ¶ 41 (“Defendants’ malware was designed to
23 give defendants and their customers access to information and data on the target
24 devices, including their communications.”).

25 Plaintiffs also pointed out at the hearing that their first cause of action under 18
26 U.S.C. § 1030 expressly includes as an element that the defendant “accesses a
27 computer” and “thereby obtains information.” 18 U.S.C. § 1030(a)(2).

28 Defendants’ proposal of producing information showing the functionality of only the

1 installation layer of the relevant spyware would not allow plaintiffs to understand how the
2 relevant spyware performs the functions of accessing and extracting data, and thus, the
3 court directs defendants to provide information sufficient to show the full functionality of
4 all relevant spyware. Under Richmark, that information is sufficiently important and
5 specific such that compliance with discovery obligations may not be excused.

6 As to category (3), the court concludes that defendants need not disclose the
7 identities of their third-party clients. Plaintiffs are indeed correct in arguing that
8 defendants have raised the actions of those third-party clients as a defense, and plaintiffs
9 are permitted to discover information about what actions were taken by those third
10 parties, but plaintiffs need not discover the specific identities of the third parties in order
11 to discover what role defendants played in any use of alleged spyware. Here, the court
12 also notes that defendants have “offered to stipulate that Pegasus has been used by its
13 government customers to obtain information from target devices.” Dkt. 252 at 14.

14 As to category (4), the court concludes that defendants need not provide specific
15 information regarding the server architecture at this time. At the hearing, the court asked
16 plaintiffs’ counsel to identify what information could be gleaned from this category of
17 information, and plaintiffs pointed to the ability to understand the fuller picture of how the
18 alleged spyware functioned. Based on the information presented the court, it appears
19 that plaintiffs would be able to glean the same information from the full functionality of the
20 alleged spyware, as discussed in category (2) above.

21 Thus, overall, plaintiffs’ motion to compel discovery is GRANTED in part and
22 DENIED in part.

23 B. Defendants’ motion to compel discovery (Dkt. 240)

24 Defendants’ motion seeks two categories of documents: (1) plaintiffs’
25 communications with third-party witness Citizen Lab, and (2) plaintiffs’ internal documents
26 relating to their identification of the users allegedly targeted by defendants’ software. As
27 to (2), plaintiffs produced documents after the filing of this motion, and as stated at the
28 hearing, while the parties may still have disputes about individual documents that may be

1 resolved through the meet-and-confer process, there is no ripe dispute for the court to
2 resolve at this time.

3 As to (1), defendants argue that the Citizen Lab communications are relevant to
4 the claims and defenses asserted in this case because “plaintiffs’ central theme in this
5 case is that Pegasus is misused by NSO’s customers against ‘civil society,’ and plaintiffs
6 have specifically identified Citizen Lab as having relevant information about that core
7 allegation.” Dkt. 240 at 11.

8 Plaintiffs argue that they “have produced all communications between plaintiffs
9 and Citizen Lab relevant to Citizen Lab’s role related to the case, which occurred entirely
10 before the complaint was filed.” Dkt. 250 at 8. To the extent that defendants seek post-
11 complaint communications with Citizen Lab, plaintiffs argue that defendants have “fail[ed]
12 to explain why plaintiffs’ post-complaint communications with Citizen Lab are likely to
13 have any connection to the case.” Id.

14 The court concludes that defendants have not shown how the requested discovery
15 is warranted under Rule 26(b)(1). Defendants argue that the “core allegation” of the
16 complaint is that “Pegasus is misused by NSO’s customers against ‘civil society,’” but
17 defendants have not explained how the “civil society” allegation relates to any of the
18 specific three causes of action that remain operative in the case, or any of the specific
19 affirmative defenses asserted in response. In fact, in a footnote in their reply, defendants
20 offer that “[i]f plaintiffs would agree to withdraw from their case Citizen Lab’s contention
21 that Pegasus was used against members of ‘civil society’ rather than to investigate
22 terrorism and serious crime, there would be much less need for this discovery.” See Dkt.
23 258 at 4, n.1. It appears from that representation that the “civil society” allegation
24 appears to be an ancillary part of this case – rather than relating to one of the elements of
25 the asserted claims or defenses in this case. On that basis, the court fails to see the
26 relevance of the requested discovery, and thus, denies defendants’ motion to the extent
27 that it seeks post-complaint communications between plaintiffs and Citizen Lab.
28

