

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

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

Case No. 19-cv-07123-PJH

**ORDER RE MOTIONS FOR  
SUMMARY JUDGMENT, MOTION  
FOR SANCTIONS, AND DISCOVERY  
LETTER BRIEFS**

Re: Dkt. 381, 383, 387, 397, 401, 406,  
408, 409, 411

Plaintiffs’ motion for summary judgment, defendants’ motion for summary judgment/motion to dismiss, and plaintiffs’ motion for sanctions came on for hearing on November 7, 2024. Plaintiffs appeared through their counsel, Antonio Perez-Marques, Craig Cagney, Micah Block, Greg Andres, Gina Cora, and Luca Marzorati. Defendants appeared through their counsel, Joseph Akrotirianakis, Matthew Dawson, and Matthew Noller. Having read the papers filed by the parties and carefully considered their arguments and relevant authority, and good cause appearing, the court hereby rules as follows.

**BACKGROUND**

On October 29, 2019, plaintiffs filed this lawsuit, alleging that defendants sent malware, 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

United States District Court  
Northern District of California

United States District Court  
Northern District of California

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

3 The court dismissed plaintiffs’ fourth cause of action under Rule 12(b)(6), and no  
4 amended complaint was filed. See Dkt. 111. That leaves only the first three causes of  
5 action as operative claims in this case. The allegations underlying the complaint are set  
6 forth in detail in the court’s previous order on defendants’ motion to dismiss. See Dkt.  
7 111. As relevant to this order, the parties’ briefs further explain some technical details  
8 regarding the parties’ respective technologies. To summarize, when users communicate  
9 via plaintiffs’ software, plaintiffs use a “signaling server” to create an initial connection  
10 between two users, and then use a “relay server” to send the communication data  
11 between the parties.

12 Defendants’ relevant software products, collectively referred to as “Pegasus,”  
13 allow defendants’ clients to use a modified version of the Whatsapp application – referred  
14 to as the “Whatsapp Installation Server,” or “WIS. The WIS, among other things, allows  
15 defendants’ clients to send “cipher” files with “installation vectors” that ultimately allow the  
16 clients to surveil target users. As mentioned above, plaintiffs allege that defendants’  
17 conduct was a violation of the CFAA, the CDAFA, and a breach of contract.

18 Plaintiffs now move for partial summary judgment seeking a finding of liability on  
19 all claims, leaving only the issue of damages for trial. Defendants move to dismiss or for  
20 summary judgment based on lack of personal jurisdiction and for partial summary  
21 judgment on the merits of the asserted claims. Plaintiffs also seek sanctions based on  
22 defendants’ discovery conduct.

23 **DISCUSSION**

24 A. Legal standard

25 1. Motion for summary judgment

26 Summary judgment is proper where the pleadings, discovery, and affidavits show  
27 that there is “no genuine dispute as to any material fact and the movant is entitled to  
28 judgment as a matter of law.” Fed. R. Civ. P. 56(a). Material facts are those which may

1 affect the outcome of the case. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248  
2 (1986). A dispute as to a material fact is genuine if there is sufficient evidence for a  
3 reasonable jury to return a verdict for the nonmoving party. Id. “A ‘scintilla of evidence,’  
4 or evidence that is ‘merely colorable’ or ‘not significantly probative,’ is not sufficient to  
5 present a genuine issue as to a material fact.” United Steelworkers of Am. v. Phelps  
6 Dodge Corp., 865 F.2d 1539, 1542 (9th Cir. 1989) (citation omitted).

7 Courts recognize two ways for a moving defendant to show the absence of  
8 genuine dispute of material fact: (1) proffer evidence affirmatively negating any element  
9 of the challenged claim and (2) identify the absence of evidence necessary for plaintiff to  
10 substantiate such claim. Nissan Fire & Marine Ins. Co. v. Fritz Cos., 210 F.3d 1099,  
11 1102 (9th Cir. 2000) (“In order to carry its burden of production, the moving party must  
12 either produce evidence negating an essential element of the nonmoving party's claim or  
13 defense or show that the nonmoving party does not have enough evidence of an  
14 essential element to carry its ultimate burden of persuasion at trial.”)

15 “Once the moving party meets its initial burden, the nonmoving party must go  
16 beyond the pleadings and, by its own affidavits or by the depositions, answers to  
17 interrogatories, and admissions on file, come forth with specific facts to show that a  
18 genuine issue of material fact exists.” Hansen v. United States, 7 F.3d 137, 138 (9th Cir.  
19 1993) (per curiam). “When the nonmoving party relies only on its own affidavits to  
20 oppose summary judgment, it cannot rely on conclusory allegations unsupported by  
21 factual data to create an issue of material fact.” Id.

22 The court must view the evidence in the light most favorable to the nonmoving  
23 party: if evidence produced by the moving party conflicts with evidence produced by the  
24 nonmoving party, the judge must assume the truth of the evidence set forth by the  
25 nonmoving party with respect to that fact. See Tolan v. Cotton, 134 S. Ct. 1861, 1865  
26 (2014); Leslie v. Grupo ICA, 198 F.3d 1152, 1158 (9th Cir. 1999). However, when a non-  
27 moving party fails to produce evidence rebutting defendants’ showing, then an order for  
28 summary adjudication is proper. Nissan Fire, 210 F.3d at 1103 (“If the nonmoving party

1 fails to produce enough evidence to create a genuine issue of material fact, the moving  
2 party wins the motion for summary judgment.”

3 2. Motion for sanctions

4 Federal Rule of Civil Procedure 37(b)(2)(A) provides for sanctions for not obeying  
5 a discovery order, specifically providing that “if a party . . . fails to obey an order to  
6 provide or permit discovery . . . the court where the action is pending may issue further  
7 just orders,” including “directing that the matters embraced in the order or other  
8 designated facts be taken as established for purposes of the action, as the prevailing  
9 party claims,” or “rendering a default judgment against the disobedient party.”

10 B. Legal analysis

11 The court will first address the threshold jurisdictional issue raised by defendants’  
12 motion, and will then address the merits of the three claims asserted by plaintiffs.

13 1. Personal jurisdiction

14 Defendants’ summary judgment motion and their opposition to plaintiffs’ motion  
15 both argue that the court lacks personal jurisdiction. As an initial matter, defendants’  
16 opposition to the sanctions motion also contains a single sentence (without elaboration or  
17 citation) stating that five cases were filed against defendants, four of which have been  
18 dismissed, three of which were for lack of personal jurisdiction and/or forum non  
19 conveniens. At the hearing, the court asked defendants for clarification as to which  
20 cases they were referring. Defendants identified a case in this district that was voluntarily  
21 dismissed by Apple (case no. 21-9078), as well as three other cases:

- 22 • Corallo v. NSO, N.D. Cal. (Seeborg, J.), case no. 22-5229, dismissed on  
23 September 30, 2024 based on lack of personal jurisdiction and/or forum non  
24 conveniens, as plaintiff was a native of Italy and citizen of the Netherlands who  
25 resided in St Maarten in the Caribbean at the time of the alleged attacks. (“Corallo  
26 is a foreign citizen suing other foreign citizens for conduct initiated from foreign  
27 locations. The litigation does not belong in the courts of this state.”)
- 28 • Dada v. NSO, N.D. Cal. (Donato, J.), case no. 22-7513, dismissed on March 8,

United States District Court  
Northern District of California

1 2024 based on forum non conveniens, as plaintiffs were journalists for a  
2 newspaper based in El Salvador. (“The nub of this case is entirely foreign, and  
3 concerns the use of software produced in Israel to hack devices owned by a  
4 Salvadoran news service and used by journalists in El Salvador. Every incident  
5 described in the complaint involved Salvadoran journalists covering Salvadoran  
6 news stories while working primarily in El Salvador.”)

7 • Elatr Khashoggi v. NSO, E.D. Va., case no. 23-0779, dismissed on October 26,  
8 2023 based on lack of personal jurisdiction, as plaintiff was a citizen of Egypt and  
9 had not adequately alleged that she was in Virginia during the alleged attacks.

10 The key distinction in all of those cases appears to be the citizenship/residency of  
11 the plaintiffs. In this case, defendants do not dispute that plaintiffs are citizens of the  
12 United States and residents of this district, making the cited cases inapposite.

13 Turning to the merits of defendants’ jurisdictional argument, as was laid out in the  
14 court’s previous order at the pleadings stage, personal jurisdiction can be established  
15 through consent, or by either showing that defendants purposefully directed conduct at  
16 the forum state, or that they purposefully availed themselves of the state’s laws. See Dkt.  
17 111 at 15-32. The court’s previous order concluded that plaintiffs had adequately alleged  
18 purposeful direction, see Dkt. 111 at 28, but defendants now argue that the allegations  
19 are not supported by the evidence.

20 As to purposeful direction, the court’s previous order went through the relevant  
21 analysis, explaining that the test has three elements (1) defendants committed an  
22 intentional act, (2) expressly aimed at the forum state, and (3) caused harm that the  
23 defendant knew was likely to be suffered in the forum state. Dkt. 111 at 18 (citing Calder  
24 v. Jones, 465 U.S. 783, 789-90 (1984)).

25 The key arguments – both then and now – go to the second element, express  
26 aiming. Plaintiffs allege that defendants expressly aimed their conduct at plaintiffs’  
27 servers, a significant number of which are in California. Defendants now argue that,  
28 while the court was obligated to accept that allegation as true at the pleadings stage,

1 discovery has shown that none of plaintiffs' signaling servers are in California and only  
2 some of their relay servers are in California, and more importantly, the choice of which  
3 server to use was made by plaintiffs, and thus defendants could not have engaged in any  
4 express aiming of servers.

5 Plaintiffs argue that, because defendants did not produce Pegasus code, there is  
6 no way of confirming exactly how the WIS chose which server to use. Defendants self-  
7 servingly claim that the WIS functioned in the same way as the official Whatsapp client,  
8 but there is no evidence to support that claim. Plaintiffs also argue that, even if the WIS  
9 did indeed function in the same way, that was still an intentional choice made by  
10 defendants. See Dkt. 418-3 at 15-16.

11 The limited evidentiary record before the court does show that defendants'  
12 Pegasus code was sent through plaintiffs' California-based servers 43 times during the  
13 relevant time period in May 2019. See, e.g., Dkt. 418-3 at 13. The evidence before the  
14 court is consistent with the court's earlier conclusion, at the pleading stage, that  
15 defendants "caused a digital transmission to enter California, which then effectuated a  
16 breaking and entering of a server in California." See Dkt. 111 at 23. Accordingly, the  
17 court finds that the evidentiary record supports the conclusion that defendants are subject  
18 to personal jurisdiction in this district.

19 Because plaintiffs' argument also implicates defendants' discovery conduct, the  
20 court will now address plaintiffs' motion for sanctions.

## 21 2. Motion for sanctions

22 The crux of plaintiffs' sanctions motion is that defendants have failed to produce  
23 Pegasus source code in a manner that can be used in this litigation, failed to produce  
24 internal communications (i.e., email), and wrongfully imposed temporal limitations on their  
25 production/testimony. Plaintiffs ask for terminating sanctions, or in the alternative,  
26 evidentiary sanctions.

27 With regard to the Pegasus source code, plaintiffs point out the history of the  
28 court's orders regarding defendants' discovery obligations. In November 2023, the court

1 issued an order balancing (under Richmark) defendants' discovery obligations with its  
2 need to comply with Israeli government restrictions, and concluded that defendants would  
3 not be entirely excused from discovery, and instead would be required to produce  
4 information that was "sufficiently specific and important to the asserted claims in this  
5 case." Dkt. 233 at 9.

6 In February 2024, the court considered specific discovery disputes between the  
7 parties, one of which involved defendants' argument that they were required to produce  
8 only the "installation layer" of the source code, showing how Pegasus was installed on  
9 the target users' devices. The court rejected that argument, because "the complaint  
10 contains numerous instances alleging not only that spyware was installed on users'  
11 devices, but also that information was accessed and/or extracted from those devices."  
12 Dkt. 292 at 4 (emphasis added). Accordingly, the court held that defendants "must  
13 produce information concerning the full functionality of the relevant spyware." Id. The  
14 court went on to say:

15 Defendants' proposal of producing information showing the functionality of  
16 only the installation layer of the relevant spyware would not allow plaintiffs  
17 to understand how the relevant spyware performs the functions of  
18 accessing and extracting data, and thus, the court directs defendants to  
19 provide information sufficient to show the full functionality of all relevant  
20 spyware. Under Richmark, that information is sufficiently important and  
21 specific such that compliance with discovery obligations may not be  
22 excused.

23 Id. at 4-5.

24 Then, a few months later, plaintiffs moved to compel production of one of  
25 defendants' computer servers containing Pegasus source code (referred to as the "AWS"  
26 (Amazon web services) server). Defendants claimed that production was not warranted,  
27 arguing that the court never technically used the word "granted" in its previous order with  
28 respect to the Pegasus code. Defendants argued that they were prepared to file a  
motion for reconsideration/clarification to pursue their argument that production of source  
code was not actually required. The court instead issued an order granting plaintiffs'  
motion to compel the AWS server and "clarify[ing] that the previous order's reference to

1 'full functionality' was indeed intended to require NSO to produce Pegasus computer  
2 code." Dkt. 358 at 5-6. The court then further clarified:

3 Accordingly, the court now clarifies that its previous order, dated February  
4 23, 2024, should be read to encompass Pegasus computer code, as well as  
5 code that shows the full functionality of any other "relevant spyware." To the  
6 extent that information on the AWS server as of November 2020, and which  
7 has since been moved to a different server, reflects such computer code,  
8 the court orders production of that code under Richmark, as the information  
9 is sufficiently important and specific to require production despite the  
10 existence of foreign legal restrictions. To be clear, the court is not  
11 rebalancing the Richmark factors on this motion, it is simply reiterating the  
12 balance that was struck in the previous order. The information showing the  
13 full picture of how Pegasus functions – which squarely includes Pegasus  
14 computer code – is discoverable under Richmark despite the various  
15 restrictions that have been cited.

16 Id. at 6.

17 Plaintiffs now argue that defendants have produced Pegasus code in a manner  
18 that is unusable in this litigation, as it is viewable only by Israeli citizens while in Israel.  
19 And even that production is limited to Pegasus code that was on the one specific AWS  
20 server mentioned above, rather than the full set of Pegasus code that would show its full  
21 functionality. Plaintiffs cite cases from this district and C.D. Cal. holding that production  
22 of source code in a foreign country or "distant" or "relatively inaccessible" location was  
23 not compliant with the federal rules. See Dkt. 405 at 19-20 (citing Rambus v. Hynix, 2007  
24 WL 9653194 (N.D. Cal. 2007); Satya v. Martin, 2019 WL 666722 (N.D. Cal. 2019);  
25 InTouch Techs. v. VGO, 2012 WL 7783405 (C.D. Cal. 2012)).

26 Beyond source code, plaintiffs also argue that defendants refused to produce  
27 internal communications, including communications about Whatsapp vulnerabilities and  
28 about NSO's interactions with the US company Westbridge. Plaintiffs also argue that  
29 defendants refused to produce key financial information and refused to answer certain  
30 deposition questions.

31 As mentioned above, plaintiffs ask for terminating sanctions, and alternatively ask  
32 for evidentiary sanctions on the following topics: (1) targeting of plaintiffs' California-  
33 based servers, (2) location of third-party servers, (3) relationship with Westbridge, (4) use



United States District Court  
Northern District of California

1 of Pegasus by NSO's customers, as well as "additional issues to be determined."

2 Defendants' opposition makes a number of different arguments, including an  
3 argument that the court never ordered them to produce any Pegasus source code  
4 beyond what was on the AWS server. See, e.g., Dkt. 429-2 at 8, 17-18.

5 Defendants also argue that production of the AWS server in Israel is fully  
6 compliant with discovery obligations, as plaintiffs could either use Israeli counsel to view  
7 the code, or they could seek an export license from the Israeli government to use the  
8 code in the US.

9 Overall, the court concludes that defendants have repeatedly failed to produce  
10 relevant discovery and failed to obey court orders regarding such discovery. Most  
11 significant is the Pegasus source code, and defendants' position that their production  
12 obligations were limited to only the code on the AWS server is a position that the court  
13 cannot see as reasonable given the history and context of the case. Moreover,  
14 defendants' limitation of its production such that it is viewable only by Israeli citizens  
15 present in Israel is simply impracticable for a lawsuit that is to be litigated in this district.

16 Accordingly, the court concludes that plaintiffs' motion for sanctions must be  
17 GRANTED. And while the court concludes that terminating sanctions may be reasonably  
18 warranted given that defendants' discovery non-compliance goes to the key facts at issue  
19 in this case, the court prefers not to issue such a harsh sanction where lesser ones are  
20 available. Thus, the court will impose evidentiary sanctions when appropriate, but will  
21 only address the issue of terminating sanctions if plaintiffs are unable to establish their  
22 claims in their absence.

23 The first topic of possible evidentiary sanctions, mentioned above, is defendants'  
24 alleged targeting of plaintiffs' California-based servers. The court concludes that,  
25 because defendants did not produce Pegasus code in a way that was meaningfully  
26 accessible to plaintiffs or to the court, plaintiffs were unable to obtain detailed evidence of  
27 how the WIS chose which server(s) to use, and thus, an evidentiary sanction is warranted  
28 such that the court will conclude that the use of plaintiffs' California-based servers was a

United States District Court  
Northern District of California

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

purposeful choice made by defendants. Accordingly, the court reiterates its previous conclusion that the record supports a finding that defendants are subject to personal jurisdiction in this district.

3. Merits of the asserted claims

As mentioned above, plaintiffs assert claims for violation of the CFAA, for violation of the CDAFA, and for breach of contract.

a. CFAA

As to the CFAA, plaintiffs allege that defendants violated sections (a)(2) and (a)(4), and also conspired with their clients in violation of section (b). The relevant provisions are as follows:

(a) Whoever—

...

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

...

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.

...

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030.

1 Plaintiffs' motion also argues that defendants have violated section (a)(6), which  
2 prohibits trafficking in password-like information, but they acknowledge that they did not  
3 plead section (a)(6). See Dkt. 399-2 at 30, n. 10. Because any claim under section  
4 (a)(6) was not pled in the complaint, the court will not consider it now.

5 The first big dispute on the CFAA, briefly alluded to above, is that plaintiffs now  
6 seek to proceed under either a "without authorization" or "exceeds authorization" theory,  
7 even though the court's previous order limited them to the "exceeds authorization" theory.  
8 See Dkt. 111 at 35-39. The court reasoned that, because all Whatsapp users are  
9 authorized to send messages, defendants did not act without authorization by sending  
10 their messages, even though the messages contained spyware. Instead, the court held  
11 that the complaint's allegations supported only an "exceeds authorization" theory.

12 The nub of the fight here is semantic. Essentially, the issue is whether sending  
13 the Pegasus installation vector actually did exceed authorized access. Defendants argue  
14 that it passed through the Whatsapp servers just like any other message would, and that  
15 any information that was 'obtained' was obtained from the target users' devices (i.e., their  
16 cell phones), rather than from the Whatsapp servers themselves. (Defendants also  
17 argue that any 'obtaining' was done by their government clients, rather than by  
18 defendants, but that's a separate argument – and in the court's view, fully addressed by  
19 section (b) which assigns liability to co-conspirators).

20 Defendants point to the statutory definitions set forth in § 1030(e)(6), specifically  
21 the definition of "exceeds authorized access" as "to access a computer with authorization  
22 and to use such access to obtain or alter information in the computer that the accesser is  
23 not entitled so to obtain or alter." Defendants argue that the definition shows that the  
24 alleged violator must "obtain or alter" information from the same computer that he  
25 "access[es]," as shown by the language "the computer."

26 For their part, plaintiffs point to section (a)(2) itself, which imposes liability on  
27 whoever "accesses a computer" in excess of authorized access, and "thereby obtains  
28 information from any protected computer," pointing to the word "any."

1 Neither party cites any case law, either controlling or even persuasive, with a  
2 definitive answer to this statutory interpretation question. Plaintiffs, relying on section  
3 (a)(2)(C), argue that liability is present if defendants obtain information from any  
4 computer, i.e., either from Whatsapp servers or from the target users' devices directly.  
5 Defendants, pointing to section (e)(6), argue that any information was obtained from the  
6 target users, not from Whatsapp's servers, and thus the CFAA does not apply.

7 However, the court need not resolve this statutory interpretation question in order  
8 to rule on the summary judgment motions. As the parties clarified at the hearing, while  
9 the WIS does obtain information directly from the target users' devices, it also obtains  
10 information about the target users' device via the Whatsapp servers. See Dkt. 464 at 44  
11 ("before Pegasus is on the device, in the process of getting the Pegasus agent installed  
12 on the target device, there is a whole lot of signaling that goes on. . . . They had to  
13 fingerprint the device which used a pretty sophisticated set of messaging to get  
14 information back to the WIS via the Whatsapp servers about the precise operating  
15 system and memory structure of the [target] phone."); see also Dkt. 399-2 at 27 ("NSO  
16 also obtained information via the Whatsapp servers from the target device, such as the  
17 structure of its operating system and the location of crucial memory files, which a regular  
18 Whatsapp user using the Whatsapp client app cannot obtain.").

19 The analysis for section (a)(4) is largely the same, as it uses the same statutory  
20 definition found in section (e)(6). Plaintiffs argue that the information's value is  
21 established by defendants' clients' willingness to pay for Pegasus. Defendants challenge  
22 the mens rea showing for the 'intent to defraud' (as well as the 'intent' requirement of  
23 section (a)(2)), but the fact that defendants redesigned Pegasus to evade detection after  
24 plaintiffs first fixed the security breach is enough to prove intent.

25 Thus, the court GRANTS summary judgment in plaintiffs' favor on the CFAA claim  
26 under both section (a)(2) and (a)(4), on the theory that defendants exceeded their  
27 authorization. Defendants appear to fully acknowledge that the WIS sent messages  
28 through Whatsapp servers that caused Pegasus to be installed on target users' devices,

1 and that the WIS was then able to obtain protected information by having it sent from the  
2 target users, through the Whatapp servers, and back to the WIS. Defendants' only  
3 arguments go to statutory interpretation (addressed above), and their delegation of  
4 Pegasus operation to their clients (addressed by § 1030(b)). The court need not address  
5 plaintiffs' alternative argument, that defendants acted without authorization.

6 b. CDAFA

7 The CDAFA is the state-law equivalent of the CFAA, with the additional  
8 requirement that a computer be unlawfully accessed in California. See, e.g., Meta  
9 Platforms, Inc. v. BrandTotal Ltd., 605 F.Supp.3d 1218, 1260 (N.D. Cal. 2022). In the  
10 court's view, plaintiffs' evidence regarding California relay servers is sufficient, even  
11 without more, and to the extent the statute requires an intent to target a California server,  
12 the outcome is the same as it was with respect to the jurisdictional analysis – because  
13 defendants' failure to produce Pegasus source code is at least one reason why there is  
14 no evidence of exactly how the WIS chose servers, an evidentiary sanction is appropriate  
15 to conclude that the WIS did indeed target California servers. Thus, the court concludes  
16 that summary judgment must be GRANTED on the CDAFA claim for the same reasons  
17 as the CFAA claim.

18 c. Breach of contract

19 The elements of a breach of contract claim are (1) the existence of a contract, (2)  
20 plaintiff's performance or excused non-performance, (3) defendant's breach, and (4)  
21 resulting damages. See, e.g., EDC Techs. v. Seidel, 216 F.Supp.3d 1012, 1015 (N.D.  
22 Cal. 2016).

23 As mentioned above, the breach of contract claim is based on violation of the  
24 terms of service, specifically the provisions prohibiting users from "reverse engineering"  
25 or "decompiling" Whatsapp products, from sending "harmful code" through Whatsapp,  
26 and from collecting user information, from accessing or attempting to access Whatsapp  
27 without authorization, and from using Whatsapp for illegal purposes.

28 Defendants argue that no contract exists because there is no evidence that they

United States District Court  
Northern District of California

1 agreed to the terms of service. However, defendants cannot meaningfully dispute that  
2 agreeing to the terms of service was necessary to create a Whatsapp account and to use  
3 Whatsapp, and moreover, defendants have refused to produce information about the  
4 phones that were used to create Whatsapp accounts on defendants' behalf. See Dkt.  
5 408. Based on controlling Ninth Circuit case law regarding agreement to terms of  
6 service, the court concludes that a contract was indeed formed between plaintiffs and  
7 defendants. See, e.g., Laatz v. Zazzle, Inc., 2024 WL 377970 at \*7 (N.D. Cal. Jan. 9,  
8 2024); Sellers v. JustAnswer LLC, 73 Cal.App.5th 444, 472 (2021).

9 Defendants do not dispute that plaintiffs performed their obligations under the  
10 contract. That leaves the last two elements, breach and damages.

11 NSO offers only about two pages of opposition regarding breach. First, they argue  
12 that plaintiffs cannot prove when they reverse-engineered or decompiled the Whatsapp  
13 program, and therefore it could have been done before any agreement to the terms of  
14 service. But as plaintiffs point out, they offer no evidence as to when they did such  
15 reverse-engineering or decompiling.

16 Next, defendants argue that Pegasus was operated by their clients, and thus  
17 defendants did not collect any information. Defendants further argue that terms such as  
18 'illegal,' 'unauthorized,' and 'harmful' as used in the terms of service are vague and  
19 ambiguous. Finally, defendants argue that plaintiffs waived those contractual provisions  
20 by failing to enforce them against any other users. See Dkt. 419-2 at 15-17.

21 The court finds no merit in the arguments raised by defendants. Defendants do  
22 not dispute that they must have reverse-engineered and/or decompiled the Whatsapp  
23 software in order to develop the WIS, but simply raise the possibility that they did so  
24 before agreeing to the terms of service. However, as discussed above, defendants have  
25 withheld evidence regarding their agreement to the terms of service. Moreover, common  
26 sense dictates that defendants must have first gained access to the Whatsapp software  
27 before reverse-engineering and/or decompiling it, and they offer no plausible explanation  
28 for how they could have gained access to the software without agreeing to the terms of

1 service. Accordingly, the court concludes that plaintiffs have sufficiently established  
2 breach.

3 Finally, as to damages, defendants do not dispute that plaintiffs incurred costs  
4 investigating and remediating defendants' breaches, which are sufficient to establish the  
5 fourth and final element of a breach of contract claim. Accordingly, the court GRANTS  
6 summary judgment on plaintiffs' claim for breach of contract.

7 4. Discovery letter briefs

8 For the reasons set forth above, the court concludes that summary judgment is  
9 warranted even without resolving the disputes raised by the parties' various discovery  
10 letter briefs. Thus, the discovery letter briefs (Dkt. 381, 383, 387, 408, 409, 411) are all  
11 DENIED as moot, as is the related motion for clarification (Dkt. 404).

12 5. Motions to seal

13 At the hearing, the court stated to the parties that it would not seal the material in  
14 the parties' briefs, and directed the parties to file unredacted versions of the briefs on the  
15 public docket. See Dkt. 464 at 5-6, 94. The parties have since filed unredacted versions  
16 of the summary judgment briefs, and have filed briefs on the sanctions motion with limited  
17 redactions, with plaintiffs having filed a narrowed motion to seal based on defendants'  
18 confidentiality designations. See Dkt. 471.

19 In light of the court's decision not to seal the summary judgment briefs, the parties  
20 are now directed to meet and confer with the purpose of filing an omnibus motion to seal  
21 that would cover all material sought to be sealed in the exhibits and declarations in  
22 connection with the summary judgment motions. The parties shall have until **January**  
23 **17, 2025** to file the omnibus sealing motion. Any opposition shall be filed by **January 24,**  
24 **2025.**

25 The motion to seal the limited material in the briefing on the motion for sanctions  
26 (Dkt. 471) is GRANTED. For the exhibits and declarations filed in connection with the  
27 sanctions motion, the parties are similarly directed to meet and confer and to file an  
28 omnibus motion with the same briefing schedule as above.

