No. 25-7380

IN THE

United States Court of Appeals

FOR THE NINTH CIRCUIT

WHATSAPP INC., a Delaware corporation;
META PLATFORMS, INC., FKA FACEBOOK INC.,

Plaintiffs-Appellees,

v.

NSO GROUP TECHNOLOGIES LIMITED;
Q CYBER TECHNOLOGIES LIMITED,

Defendants-Appellants.

On Appeal from the United States District Court for the Northern District of California, No. 4:19-cv-7123-PJH, Hon. Phyllis J. Hamilton, District Judge

DEFENDANTS-APPELLANTS' REPLY BRIEF

STEPHEN A. BROOME
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
865 S. Figueroa St., 10th Floor
Los Angeles, CA 90017
(213) 443-3000

HOPE D. SKIBITSKY
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
295 5th Ave., 9th Floor
New York, NY 10016
(212) 849-7000

DEREK L. SHAFFER
RACHEL FRANK QUINTON
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
555 13th St. NW, Suite 600
Washington, DC 20004
(202) 538-8000

ALEX H. LOOMIS
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
111 Huntington Ave., Suite 520
Boston, MA 02199
(617) 712-7100

Counsel for Defendants-Appellants
NSO Group Technologies Limited and Q Cyber Technologies Limited

July 1, 2026

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES ii
INTRODUCTION 1
ARGUMENT 3
I. WHATSAPP CANNOT DEFEND THE SUMMARY JUDGMENT RULING 3
A. The CFAA/CDAFA Claims Turn On Disputed Facts 3
1. NSO Did Not Circumvent Access Controls When Sending Messages To WhatsApp's Servers 4
2. WhatsApp Did Not Revoke Access To Its Servers 8
3. NSO Did Not Access Third Parties' Phones 10
B. The Contract Claim Turns On Disputed Facts 14
II. WHATSAPP CANNOT DEFEND THE PERMANENT INJUNCTION 16
A. The Injunction Is Not Needed To Prevent Irreparable Harm 16
B. The Injunction Will Destroy NSO 19
C. The Injunction Will Harm The Public 19
D. The Injunction Is Overbroad 22
III. WHATSAPP CANNOT DEFEND THE PUNITIVE DAMAGES AWARD 26
A. NSO's Intent Evidence Was Wrongly Excluded 26
B. The 9:1 Punitives Ratio Violated Due Process 29
CONCLUSION 32
CERTIFICATE OF COMPLIANCE 34
CERTIFICATE OF SERVICE 35

TABLE OF AUTHORITIES

Page(s)

Cases

Abrasic 90 Inc. v. Weldcote Metals, Inc.,
364 F. Supp. 3d 888 (N.D. Ill. 2019).....16

AK Futures LLC v. Boyd St. Distro, LLC,
35 F.4th 682 (9th Cir. 2022).....18, 24

Ambrosetti v. Oregon Cath. Press,
151 F.4th 1211 (9th Cir. 2025).....14

BMW of N. Am., Inc. v. Gore,
517 U.S. 559 (1996).....29

Chabolla v. ClassPass Inc.,
129 F.4th 1147 (9th Cir. 2025).....15

Cisco Sys., Inc. v. Doe I,
— U.S. —, slip op. (2026).....11, 22, 25

Dodd v. Hood River Cnty.,
59 F.3d 852 (9th Cir. 1995).....13

eBay Inc. v. MercExchange, L.L.C.,
547 U.S. 388 (2006).....16, 17

Epic Games, Inc. v. Apple, Inc.,
67 F.4th 946 (9th Cir. 2023).....16

Facebook, Inc. v. Power Ventures, Inc.,
844 F.3d 1058 (9th Cir. 2016).....9, 10, 11, 25

United States v. Fernández-Santos,
176 F.4th 120 (1st Cir. 2026) 4

Garcia v. Google, Inc.,
786 F.3d 733 (9th Cir. 2015).....19

Godun v. JustAnswer LLC,
135 F.4th 699 (9th Cir. 2025).....14, 15

Est. of Hill ex rel. Grube v. NaphCare, Inc.,
2025 WL 1588738 (9th Cir. June 5, 2025).....30

Hardeman v. Monsanto Co.,
997 F.3d 941 (9th Cir. 2021).....31

Harrington v. Cracker Barrel Old Country Store, Inc.,
142 F.4th 678 (9th Cir. 2025).....13

hiQ Labs, Inc. v. LinkedIn Corp.,
31 F.4th 1180 (9th Cir. 2022)..... 1, 6, 9, 19

United States v. Johnson,
89 F.4th 997 (7th Cir. 2024).....26

Lompe v. Sunridge Partners, LLC,
818 F.3d 1041 (10th Cir. 2016).....29

McComb v. Jacksonville Paper Co.,
336 U.S. 187 (1949).....22

Meta Platforms, Inc. v. BrandTotal Ltd.,
605 F. Supp. 3d 1218 (N.D. Cal. 2022).....10

Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.,
518 F. Supp. 2d 1197 (C.D. Cal. 2007).....18

Nelson v. City of Davis,
571 F.3d 924 (9th Cir. 2009).....5

United States v. Nosal,
844 F.3d 1024 (9th Cir. 2016).....9

Oracle USA, Inc. v. Rimini St., Inc.,
81 F.4th 843 (9th Cir. 2023)..... 22, 23, 24

Philip Morris USA v. Williams,
549 U.S. 346 (2007).....30

Plata v. Lands' End, Inc.,
2025 WL 2408818 (9th Cir. Aug. 20, 2025).....14

United States v. Ponce,
22 F.4th 1045 (9th Cir. 2022).....23

Ramirez v. TransUnion LLC,
951 F.3d 1008 (9th Cir. 2020).....31

Riley v. Volkswagen Grp. of Am., Inc.,
51 F.4th 896 (9th Cir. 2022).....29

United States v. Roldan,
167 F.4th 569 (2d Cir. 2026).....26

Est. of Saunders v. C.I.R.,
745 F.3d 953 (9th Cir. 2014).....7

Shirk v. United States ex rel. Dep't of Interior,
773 F.3d 999 (9th Cir. 2014).....3

Sidibe v. Sutter Health,
103 F.4th 675 (9th Cir. 2024).....25, 28

Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa, 482 U.S. 522 (1987).....27

S. Union Co. v. Irvin,
563 F.3d 788 (9th Cir. 2009).....30

Starbucks Corp. v. McKinney,
602 U.S. 339 (2024).....20

State Farm Mut. Auto. Ins. Co. v. Campbell,
538 U.S. 408 (2003).....30, 31

United States v. U.S. Gypsum Co.,
340 U.S. 76 (1950).....22, 23, 25

Van Buren v. United States,
593 U.S. 374 (2021).....1, 6, 8, 9, 10

In re V.V.,
51 Cal. 4th 1020 (2011).....26

Statutes

18 U.S.C. § 1030(a)(2).....11

18 U.S.C. § 1030(e)(6).....3, 11

Cal. Civ. Code § 3294(a) 27

Cal. Civ. Code § 3294(c)(1).....27

Cal. Penal Code § 502(c) 11

Cal. Penal Code § 502(d)(1).....31

Rules

Fed. R. Civ. P. 37.....27

Fed. R. Evid. 401 ..... 12, 26

Fed. R. Evid. 403 ..... 26, 28

Other Authorities

Don't Panic. Making Progress on the "Going Dark" Debate, Berkman Ctr. for Internet & Soc. (Feb. 1, 2016).....21

Madeline Earp, *How Vietnam-based hacking operation OceanLotus targets journalists*, Comm. to Protect Journalists (Feb. 1, 2021).....13

Mark Mazzetti & Ronen Bergman, *Internal Documents Show How Close the F.B.I. Came to Deploying Spyware*, N.Y. Times (Nov. 12, 2022).....21

Statement from John Brennan, Assistant to the President for Homeland Security & Counter-Terrorism, White House (Oct. 29, 2010) 20

Steve M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 1 (2014).....12

"WhatsApp Statistics and Insights," Armin (May 8, 2026) 25

Yinon Ben Shushan, *WhatsApp, YouTube, and Facebook: What are the most popular apps used in Israel in 2025?*, Jerusalem Post (Oct. 6, 2025).....24

INTRODUCTION

Unable to defend the district court's actual reasoning, WhatsApp runs from it, all but confessing error below. Over the span of 27 pages purporting to justify the grant of summary judgment, WhatsApp cites the actual reasoning below exactly twice (AB.42-43, 47). By any reading, WhatsApp hopes to persuade this Court to affirm on alternative grounds, as spun on appeal. But the fact-intensive, highly technical, hotly contested questions on which this case turns are wholly insusceptible to summary judgment, much less summary judgment granted via appellate review. The warrant for vacating and remanding is apparent.

On the CFAA/CDAFA claims, WhatsApp does not defend the district court's ruling that WhatsApp violated the law by obtaining information "via WhatsApp servers." It acknowledges (AB.29) that *Van Buren v. United States*, 593 U.S. 374 (2021), imposes a gates-up/gates-down test that the district court never applied. Instead, WhatsApp now argues that NSO bypassed authentication gates by devising a fake WhatsApp client that communicated with WhatsApp servers. That is false, and at a minimum it is controverted on this record. Notably, the district court itself was unclear "about how exactly the relevant attacks were conducted." 2-ER-308. WhatsApp also alleges that NSO made WhatsApp accounts when it knew it lacked permission to do so. *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1197-202 (9th Cir. 2022), squarely forecloses this argument for online services open to the public,

like WhatsApp. WhatsApp then accuses NSO of *itself* hacking the phones of 1,400 activists and journalists. But not a shred of evidence substantiates this claim.

On the contract claim, WhatsApp does not dispute that the district court was obligated to analyze whether its terms of service were conspicuous and failed to do so. WhatsApp resorts to citing new evidence never considered below, likely because it was improperly withheld in discovery, and asks this Court to resolve the issue in the first instance. This is improper and cannot precede resolution of NSO's evidentiary objections below.

As to the injunction, WhatsApp repeatedly mischaracterizes it. The injunction is not limited to prohibiting unlawful access to WhatsApp servers and users. It expressly prohibits reverse-engineering software *on NSO's own phones and computers*, and other lawful conduct. Lawful conduct cannot be banned unless doing so is essential to protect the plaintiff from irreparable harm. WhatsApp does not even purport to meet that burden. It also claims that mere computer intrusions inherently pose irreparable harm, but that is foreclosed by numerous precedents.

Finally, faced with an oppressive 9:1 punitive damages award tainted by evidentiary exclusions, WhatsApp does not defend the district court's legally erroneous ruling that punitive damages should be higher because WhatsApp is wealthier. It instead asks this Court to fill gaps in the district court's reasoning while

deferring to the jury's verdict. The former is improper for a trial this Court did not witness, and the latter contravenes precedent.

ARGUMENT

I. WHATSAPP CANNOT DEFEND THE SUMMARY JUDGMENT RULING

A. The CFAA/CDAFA Claims Turn On Disputed Facts

WhatsApp does not challenge the district court's ruling that, as a matter of law, NSO did not access WhatsApp's servers "without authorization." 1-ER-63. That leaves it conceding that CFAA/CDAFA liability hinges on whether NSO "exceed[ed] authorized access" (AB.23) to a "computer," 18 U.S.C. § 1030(e)(6); *see* OB.27-28.

Scarcely defending the court's stated rationale—that obtaining "information about the target users' devices *via the WhatsApp servers*" is itself a CFAA/CDAFA violation absent a separate showing that NSO circumvented closed gates and accessed a protected server (OB.29-30)—WhatsApp advances its own alternative rationales. But the record refutes WhatsApp's arguments and, at minimum, shows summary judgment was granted despite genuine issues of material fact. Especially when novel, important precedent stands to be set and legal questions are inextricably intertwined with technical questions, each subject to intensive dispute, this Court should not itself grant summary judgment on any ground different from the court below. *See, e.g.*, *Shirk v. United States ex rel. Dep't of Interior*, 773 F.3d 999, 1007

(9th Cir. 2014); *United States v. Fernández-Santos*, 176 F.4th 120, 127 (1st Cir. 2026).

1. NSO Did Not Circumvent Access Controls When Sending Messages To WhatsApp's Servers

WhatsApp first contends (AB.31) that NSO exceeded authorized access to its servers by creating a "modified client application (the WIS) capable of generating attack messages that" an ordinary WhatsApp user "could not send." It asserts that these messages "were sent to WhatsApp servers by" the NSO application, "not by the official WhatsApp client" (i.e., the WhatsApp "app" that anyone can download from the app store); that sending such messages required the NSO application to use "authentication keys" to connect to the WhatsApp servers (AB.30-31); and that NSO used this access to obtain information from WhatsApp's own servers and from the phones of third parties targeted by NSO's clients (AB.39-42).

Not so. Pegasus sent messages to WhatsApp servers *via the official WhatsApp client*, and no access controls were circumvented. NSO's R&D Director, Tamir Gazneli, attested that the WhatsApp Installation Server ("WIS") is an NSO server that "*would compose messages*." 2-ER-138 (emphasis added). Those messages were sent "over WhatsApp, using a *genuine WhatsApp client and genuine WhatsApp credentials*." *Id.* (emphasis added). This aligns with, and does not contradict (*contra* AB.31 n.4), Mr. Gazneli's deposition testimony, where he explained that a "genuine WhatsApp client on the source side of th[e] transmission," created by NSO's White

Services Department, sends the message "through th[e] WhatsApp client." SER-17; *see* 3-ER-385. This testimony is not, unlike WhatsApp's case (AB.31 n.4), a post-hoc sham. In the deposition passage that WhatsApp highlights (AB.31), the "client that NSO developed" refers to "WIS," SER-14 (161:16-162:3), which again merely generates messages without sending them to WhatsApp servers. But even if Mr. Gazneli's testimony were "contradictory" (it is not), that would create "a genuine issue of material fact." *Nelson v. City of Davis*, 571 F.3d 924, 929 (9th Cir. 2009).

Nor does the record support WhatsApp's claim (AB.29) that its "servers are engineered to accept only communications generated by the official [WhatsApp] client." In the page-range cited, WhatsApp's corporate representative explains that, whenever anyone makes a WhatsApp account, a "private key" is "generated locally by the client device." SER-148. The WhatsApp servers are engineered to accept only that private key, regardless of whether it comes from an official WhatsApp application. *Id.*

WhatsApp thus errs when it characterizes (AB.34) NSO as arguing "that any hack that succeeds must be lawful because the relevant technological barriers failed to stop it." Pegasus did not circumvent "the client-authentication gate" (AB.33). WhatsApp's server gates were up for all message traffic from genuine WhatsApp applications/keys.

NSO did not "bypass[]" a technical gate on the WhatsApp servers by "extracting authorization keys from the official client" either (AB.30). The private key "never leave[s]" the client device, SER-148, and so NSO "extracted" the keys "from the SIM card" on NSO's own phones, SER-25.

Obtaining NSO's own keys from NSO's own SIM cards on NSO's own phones is not akin to using "stolen credentials" (AB.34-35) and does not violate the CFAA/CDAFA. NSO had authority to access its own phones (OB.34 n.1), and WhatsApp does not dispute this (AB.26). To be sure, the terms of service may have barred reverse-engineering (*e.g.*, AB.6), but such "contract-based" restrictions on software *downloaded on your own phone* to obtain your own keys or generate novel content does not give rise to CFAA/CDAFA liability. *hiQ*, 31 F.4th at 1196. A teenager who jailbreaks iPhone software has not engaged in "conduct analogous to 'breaking and entering.'" *Id.* at 1197 (citation omitted); *see, e.g.*, *Van Buren*, 593 U.S. at 394 (warning against interpretations that would imply "millions of otherwise law-abiding citizens are criminals"). One cannot break and enter one's own property.

That principle disposes of WhatsApp's argument (AB.31 n.4) that NSO improperly manipulated the software of WhatsApp applications on NSO's phones to cause them to send messages that the apps could not generate. This is software modification on NSO's own devices.

WhatsApp also misleads by suggesting this Court can affirm based on "evidentiary sanctions." Those sanctions went solely to NSO's personal jurisdiction defense, *not the CFAA/CDAFA merits ruling*. 1-ER-61-62; *see* 1-ER-62-65.[1] This Court should not affirm on a sanction never imposed.

Last, WhatsApp's footnoted alternative response (AB.31 n.4)—that Pegasus violated the CFAA/CDAFA when WIS created "the attack messages," even if those messages are sent by real WhatsApp clients, without circumventing technical gates—is (1) forfeited, *see, e.g.*, *Est. of Saunders v. C.I.R.*, 745 F.3d 953, 962 n.8 (9th Cir. 2014); (2) not ruled on below, and (3) wrong. That a standard WhatsApp application purportedly "could not generate attack messages" without WIS assistance does not mean that NSO exceeded access *to WhatsApp servers*. Mr. Gazneli attested, without contradiction, that the WhatsApp client application did not "prevent[], through any technological restriction or limitation, the messages sent by Pegasus from being sent to target devices." SER-18. The generated messages were not sent by an ordinary application only in the sense that they "contained code created by NSO"—proprietary code to which ordinary users lacked access. *Id.* Even if this Court were not to credit Mr. Gazneli (notwithstanding that NSO need establish only a dispute of fact), WhatsApp's argument boils down again to the notion that

[1] NSO actually made its code available for review in Israel, 1-ER-61, but the court's error here is inconsequential because its jurisdictional ruling is not at issue.

NSO bypassed restrictions on *software on NSO's own phones*, for which NSO had authorization, not technical gates on anyone else's computer.

Summary judgment was at minimum improper because the facts are disputed. Again, the district court has acknowledged that the "record did not show … specific details about how exactly the relevant attacks were conducted," 2-ER-308—a gap that goes beyond just "some implementation details" (AB.35). WhatsApp recognizes as much, hence its pivot (AB.42) to blaming evidentiary gaps on purported discovery deficiencies. The gaps result from WhatsApp's resort to alternative grounds after the actual grant of summary judgment proved indefensible.

2. WhatsApp Did Not Revoke Access To Its Servers

Similarly misconceived is WhatsApp's second alternate ground for affirmance (AB.36)—that "[e]ven if NSO had initially possessed some form of authorization, it exceeded that authorization by continuing to access WhatsApp servers after WhatsApp revoked permission." CFAA/CDAFA "liability … stems from a gates-up-or-down inquiry—one either can or cannot access a computer system, and one either can or cannot access certain areas within the system." *Van Buren*, 593 U.S. at 390. No such access occurred here. WhatsApp says (AB.36-37) that NSO made new Pegasus vectors after WhatsApp servers returned "error codes" for the old ones. That shows only that WhatsApp closed one gate, but not all open

gates, and NSO walked through an open one without circumventing any access controls, *see supra*, Part I.A.1.

WhatsApp summarily cites (AB.37-38) *Facebook, Inc. v. Power Ventures, Inc.*, 844 F.3d 1058 (9th Cir. 2016), and *United States v. Nosal*, 844 F.3d 1024 (9th Cir. 2016), but this Court has questioned and limited both cases since *Van Buren*. They control only when "authorization generally is required and has either never been given or has been revoked"—meaning that the defendant accessed computers "without authorization." *hiQ*, 31 F.4th at 1199. But, having lost on its "without authorization" theory below without reviving it here, 1-ER-63, WhatsApp cannot rely on this "without authorization" precedent.

Nosal and *Power Ventures* also "do not control" a case like this one where access to WhatsApp is "presumptively open to all comers." *hiQ*, 31 F.4th at 1199 (citation omitted). WhatsApp's 30(b)(6) designee admitted that "literally anybody could sign up for a WhatsApp account" for free, without even giving a real "name." FER-34-35.

Moreover, *hiQ* held that a public website that sends a "cease-and-desist letter" expressly revoking access does not render "further … use of" that website a CFAA violation. 31 F.4th at 1195. This case is even easier because WhatsApp never sent a cease-and-desist letter, and its complaint does not purport to revoke access. 3-ER-473-87. Nor does it matter that WhatsApp deployed "security updates that blocked"

the Pegasus installation vector and "disabled NSO-related accounts" (AB.36-37). The CFAA does not prohibit accessing an online service "made available to the public without any authentication requirement in at least the first instance, even if the owner employs technological measures to block specific users, [or] suspicious activity …." *Meta Platforms, Inc. v. BrandTotal Ltd.*, 605 F. Supp. 3d 1218, 1262 (N.D. Cal. 2022) (internal citation omitted). Last, *Power Ventures* hinged on a finding that the defendant *knew* it was not authorized to access Facebook. *See* 844 F.3d at 1066-67. The court made no such findings here.

By no means should this Court race to affirm on an alternate factually contested ground that rests on a "without authorization" theory that was rejected below, is not pressed here, and is incompatible with *Van Buren*'s technical gates-up/gates-down test.

3. NSO Did Not Access Third Parties' Phones

WhatsApp misreads NSO's brief when it says (AB.26) that "NSO admits that it accessed target devices—without any customer involvement." To the contrary, "NSO never accessed third parties' devices"; all devices "belonged to NSO with proper authorization." OB.34 n.1; 2-ER-83-84; 2-ER-126. WhatsApp does not purport to show that any of the supposed "1,400 WhatsApp attacks" were conducted by NSO (AB.26).

WhatsApp's claim (AB.27) that NSO "controlled" Pegasus during its clients' operations is not supported by its record citation (2-ER-119; 2-ER-138) or anything else (at minimum, it is factually disputed). The court ruled that "neither party," including NSO, knew "which NSO customers were responsible." 1-ER-36. That distinguishes this case from *Power Ventures*, where the defendant "acknowledged that *it* took, copied, or made use of data" without permission. 844 F.3d at 1067 (emphasis added).

Absent such control, NSO cannot be held liable for having "designed" Pegasus (AB.27). The CFAA and CDAFA impose penalties on "[w]hoever" (the person committing the act) "intentionally access[es] a computer with authorization and … use[s] such access to obtain or alter information in the computer." 18 U.S.C. § 1030(a)(2), (e)(6); *see* Cal. Penal Code § 502(c). NSO did not itself intentionally access and obtain information from third-party devices. The record also reflects that "Pegasus eventually delivers the data to the customers" without NSO involvement. SER-9.

WhatsApp is effectively injecting into the statute aiding-and-abetting civil liability, contrary to Supreme Court precedent. OB.35; *see Cisco Sys., Inc. v. Doe I*, — U.S. —, slip op. 13 (2026) (Statutory "silence is enough to" foreclose aiding-and-abetting liability). The Knight *Amicus*'s invocation (at 14) of conspiracy liability is beside the point because that provision carries additional elements that, WhatsApp

and the district court do not contest, are not met here. OB.34-35. And whether or not Knight's citation-less speculation (at 15) that spyware manufacturers "are typically intimately involved in the actual use of their products" is generally true, it is untrue here—and certainly unproven.[2] Notably, Knight relies (at 14-15) only on pleadings-stage cases—not post-discovery cases like this one.

WhatsApp's "thief" analogy (AB.28) is likewise off base. It accuses NSO of designing software that can be mis-used by its customers simply by pressing a button. The same may be said of firearms, but those manufacturers are not liable for everything their customers do.

WhatsApp's reading would also prohibit companies from developing software tools for the U.S. government and foreign allies, which "routinely use surveillance tools similar to Pegasus … purchased from private companies." 3-ER-401. The CFAA's "limited exception … for U.S. law enforcement" (AB.3) protects only "activity of a [U.S.] law enforcement [or intelligence] agency," not the companies that would be barred from developing tools for U.S. government uses. Holding that software development is a CFAA violation might also undermine Internet security, as all "software tools that exploit vulnerabilities are inherently dual use," used by both hackers and "defenders and researchers." Steve M. Bellovin,

[2] The passage Knight cites (at 15) shows only that the "system" chooses "which vector [to] use," not that NSO controls or participates in selecting third-party targets. SER-45 (actual deposition).

Matt Blaze, Sandy Clark & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 1, 62 (2014). Companies will think twice before developing tools for identifying vulnerabilities if prosecution or lawsuits might follow whenever the tools fall into the wrong hands. *See, e.g.*, Madeline Earp, *How Vietnam-based hacking operation OceanLotus targets journalists*, Comm. to Protect Journalists (Feb. 1, 2021), https://perma.cc/UF5V-EMR2 (Vietnam repurposed a legitimate "penetration testing tool" for "surveillance").

Finally, endorsing this new theory would improperly grant WhatsApp "more extensive" relief than it received below. *Dodd v. Hood River Cnty.*, 59 F.3d 852, 864 (9th Cir. 1995). The district court's specific personal jurisdiction ruling corresponded with its merits theory: NSO "expressly aimed their conduct at plaintiffs' [California] servers." 1-ER-57; *see* 1-ER-64 (NSO "obtains information … via the Whatsapp servers."). Holding, by contrast, that designing and/or controlling software *in Israel* constitutes a CFAA violation, regardless of whether NSO targeted WhatsApp servers, would sever any tie between WhatsApp's claim and NSO's forum contacts. *E.g.*, *Harrington v. Cracker Barrel Old Country Store, Inc.*, 142 F.4th 678, 685 (9th Cir. 2025) (citation omitted) (requiring forum-related contacts to be related to the suit). Given that the district court first articulated WhatsApp's software-design theory in one sentence in its post-summary judgment

clarification order, 2-ER-308-09, this Court should not affirm on this anomalous alternative ground.

B. The Contract Claim Turns On Disputed Facts

WhatsApp neither mentions nor denies that terms-of-service contract formation is a "fact-intensive" inquiry, "informed by the 'totality of the circumstances.'" *Godun v. JustAnswer LLC*, 135 F.4th 699, 709 (9th Cir. 2025) (citation omitted); *see* OB.36-37. Without denying that the court below failed to conduct the prescribed inquiry, WhatsApp urges this Court to conduct this analysis in the first instance. *See* AB.43-48. Again, this is improper, *supra*, Part I.A.2., and grounds alone to vacate.

WhatsApp's arguments are also unpersuasive. It refers (AB.44-45) to screenshots (SER-5) that the court never considered. 1-ER-65-66. WhatsApp attached the screenshots to an expert declaration submitted with its reply brief, and NSO timely objected to the declaration's admissibility because WhatsApp failed to produce or disclose this evidence in discovery, thereby denying NSO any opportunity to respond. FER-19-22; FER-25-31; *see, e.g.*, *Ambrosetti v. Oregon Cath. Press*, 151 F.4th 1211, 1220 (9th Cir. 2025) (affirming summary judgment order that excluded documents not produced in discovery). NSO could not test, for example, whether the terms-of-service hyperlink was working, a potential factual dispute precluding summary judgment. *See, e.g.*, *Plata v. Lands' End, Inc.*, No. 25-

328, 2025 WL 2408818, at *1 (9th Cir. Aug. 20, 2025). At minimum, this Court should not affirm based on evidence the court never considered and that was subject to unadjudicated challenges.

The fact that WhatsApp could supply these screenshots, however, does belie its suggestion (AB.47) that the lack of conspicuousness evidence resulted from NSO failing "to produce information" (quoting 1-ER-66).

Absent conspicuousness, WhatsApp's argument (AB.46) that NSO "created at least fifty WhatsApp accounts" is irrelevant. Again, contract law requires *both* "mutual assent" *and* "notice of the agreement." *Chabolla v. ClassPass Inc.*, 129 F.4th 1147, 1154 (9th Cir. 2025) (cleaned up); OB.36-38. It is no answer for WhatsApp to observe (AB.46) that "conspicuousness analyses typically arise when evidence puts conspicuousness in doubt." "[R]easonably conspicuous notice" is an element that WhatsApp, as the moving party, had to prove—not an affirmative defense. *Godun*, 135 F.4th at 709, 711. Regardless, NSO did put conspicuousness into doubt by contending that there was "no evidence that it agreed to the terms of service." 1-ER-65-66.

Last, the record refutes WhatsApp's assertion (AB.48-49) that NSO had "actual knowledge" of the terms of service. WhatsApp cites to SER-23-24, in which Mr. Gazneli states outright "I didn't read the terms of service." That is not knowledge.

II. WHATSAPP CANNOT DEFEND THE PERMANENT INJUNCTION

WhatsApp concedes (AB.49 & n.8) that the permanent injunction must be vacated if this Court vacates the CFAA/CDAFA summary judgment ruling, as it should, *supra*, Part I. WhatsApp fails to rebut NSO's other arguments.

A. The Injunction Is Not Needed To Prevent Irreparable Harm

WhatsApp agrees (AB.56) that "the mere fact of a statutory violation" does not establish irreparable harm. Yet that was the court's first reason for finding irreparable harm. 1-ER-12; OB.40-41. More is needed.

That leaves WhatsApp trying desperately to recast the district court's revisionist reputational-harm ruling. 1-ER-15-17; OB.41-42. By WhatsApp's account (AB.56), the court held that "computer hacking" constitutes irreparable harm because it violates "property rights." This new theory is WhatsApp's invention, however, and is infirm. Patent and copyright infringement also interfere with property rights, but infringement of those rights does not "automatically" trigger injunctive relief. *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 392-93 (2006). CFAA injunctions can issue only if necessary "to protect [the plaintiff] from future 'damage' or 'loss.'" *Abrasic 90 Inc. v. Weldcote Metals, Inc.*, 364 F. Supp. 3d 888, 908 (N.D. Ill. 2019). WhatsApp claims (AB.58) that *Epic Games, Inc. v. Apple, Inc.*, 67 F.4th 946, 1003 (9th Cir. 2023), holds that "concealed" computer intrusions "are inherently difficult to quantify," but the case bears no such gloss.

Epic is a Sherman Act case that had nothing to do with computer intrusions. *Id.* at 966.

WhatsApp also does not claim that NSO intruded on private WhatsApp computers, obtained valuable WhatsApp information, or caused it to suffer any other sort of privacy harm. Its third-party access theory (*supra*, Part I.A.3) implicates WhatsApp users' property rights, not WhatsApp's; and WhatsApp does not contend that NSO obtained *private* information from WhatsApp's own servers. Again, all Pegasus obtained from WhatsApp's servers was the same information available to all users: data about others' devices' operating systems and online status. 2-ER-123; 2-ER-128-29. WhatsApp misleadingly responds (AB.40) that "NSO's head of R&D [Mr. Gazneli] testified that Pegasus retrieved information … that 'a regular WhatsApp user using the WhatsApp client app cannot obtain'" (quoting SER-36). In fact, Mr. Gazneli replied that regular users could obtain this information "by other means on the device." SER-36. Nor does this WhatsApp-server-access theory implicate substantial property concerns. WhatsApp's own documents state that "WhatsApp servers were not compromised by" Pegasus, 2-ER-346, nor was any WhatsApp data "alter[ed], delete[d], impair[ed], or corrupt[ed]," 2-ER-150.

Part and parcel of these record deficiencies, WhatsApp has not shown that damages would be insufficient or "difficult to quantify" (AB.58). It *was* able to quantify its actual damages as $444,719, equal to WhatsApp's labor cost in patching

each exploit employed. FER-7-8. And again, reputational damages were hard to calculate only because WhatsApp waived them, precluding it from claiming that damages would be inadequate. OB.44-45.

WhatsApp lacks any other viable theory of irreparable harm (AB.50-55). It cites the same evidence as the district court that NSO designs software to help governments circumvent encryption—as is true of any company that designs similar software for U.S. government uses. But it does not dispute that this, without more, is not a CFAA/CDAFA violation, and NSO testified it would comply with the court's ruling. OB.41-43. WhatsApp asks (AB.54) this Court to find that NSO's representations are not credible, but no such finding was made. This is unlike *AK Futures LLC v. Boyd St. Distro, LLC*, 35 F.4th 682, 694 (9th Cir. 2022), and *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, 518 F. Supp. 2d 1197, 1219 (C.D. Cal. 2007) (cited AB.53, 59), where the defendants could not stop third-party trademark and copyright violations. NSO, by contrast, need only stop using WhatsApp vectors to comply with the order, and WhatsApp offers no reason to doubt NSO can do so while accomplishing its business objectives.

Last, WhatsApp claims (AB.54-55) it need show only that NSO will "exploit WhatsApp's infrastructure," in broad strokes, not that such exploits will violate the CFAA/CDAFA. That, too, is wrong: As detailed *infra*, Part II.D, a court cannot enjoin legal conduct unless doing so imposes no more burden than absolutely

necessary. None of the cited cases instructs otherwise. To the contrary, *Garcia v. Google, Inc.*, 786 F.3d 733, 744-46 (9th Cir. 2015) (en banc), denied injunctive relief because the irreparable harm did not "stem from copyright" violations. The same mismatch occurs here. WhatsApp seeks to prevent broader business and reverse-engineering harms through a "criminal hacking statute" aimed solely at unauthorized access. *hiQ*, 31 F.4th at 1201.

B. The Injunction Will Destroy NSO

WhatsApp does not dispute that the injunction threatens to drive NSO out of business, which constitutes irreparable harm, *hiQ*, 31 F.4th at 1188, or that this exceeds the risk it faces, OB.47-48. It instead says (AB.59) that the court rightly discounted NSO's destruction because this harm was "caused by illegal conduct" (citation omitted). But even if the methods NSO previously employed when developing its software violated the CFAA/CDAFA (and they did not), the injunction goes far beyond that by preventing NSO from reverse-engineering software on its own phones. Because that conduct and developing software generally are both legal, *supra*, Part I.A; *infra*, Part II.D, destroying NSO's business is inequitable.

C. The Injunction Will Harm The Public

WhatsApp wrongly argues (AB.60-61) that winning on liability automatically means an injunction is in the public interest—regardless of the collateral harms.

That, however, is not the law. A court cannot use success-on-the-merits as a substitute for "the traditional four-factor test," *Starbucks Corp. v. McKinney*, 602 U.S. 339, 346 (2024)—especially not when the injunction bans lawful conduct, *infra*, Part II.D. What WhatsApp derides (AB.62) as "generalized policy arguments" is the fact-based public interest test that squarely governs.

Strikingly, WhatsApp does not dispute that the court made an evidentiary error when it discounted testimony by Colonel Shepard and Mr. Minkler that the injunction would inhibit U.S. allies from proper law enforcement and intelligence operations. It instead claims (AB.61-62) this is irrelevant because Congress exempted the CFAA's reach only from "domestic law enforcement use." That again conflates the merits with the public interest. The public interest disfavors an injunction that would make it impossible for NSO to provide software to U.S. allies for legitimate national security operations. The upshot injures both those allies and the United States, which often depends on other countries for life-saving intelligence. *See, e.g.*, Statement from John Brennan, Assistant to the President for Homeland Security & Counter-Terrorism, White House (Oct. 29, 2010), https://perma.cc/D5KV-VC2F (crediting Saudi Arabia for stopping a terrorist attack).

Moreover, regardless of whether U.S. agencies used Pegasus in the past, they may wish to in the future. The FBI has reserved the right to deploy tools "similar"

to Pegasus. Reply Brief at 2, *N.Y. Times Co. v. U.S. Dep't of Justice*, No. 22-cv-1539, Dkt. 22 (S.D.N.Y. Nov. 1, 2022). That NSO is presently on the Entity List (AB.62) does not mean it always will be, nor does it prevent U.S. agencies from using Pegasus. *Cf.* Mark Mazzetti & Ronen Bergman, *Internal Documents Show How Close the F.B.I. Came to Deploying Spyware*, N.Y. Times (Nov. 12, 2022), https://perma.cc/AF4J-29LW (FBI came close to deploying Pegasus "in its own criminal investigations."). It should remain up to the U.S. government, not WhatsApp, to decide whether to use NSO's products.

Amici emphasize the benefits of encryption, but this is irrelevant. NSO is not weakening encryption standards; it provides a discrete pathway for governments to access encrypted data, something all governments, including the United States and its allies, can and must do in appropriate circumstances. A key authority on which *Amici* rely makes this very point. *See Don't Panic. Making Progress on the "Going Dark" Debate*, Berkman Ctr. for Internet & Soc., 9 (Feb. 1, 2016), https://perma.cc/4HSJ-MSGV ("[E]ncryption does not prevent intrusions at the end points, which has increasingly become a technique used in law enforcement investigations."). *Amici* also warn of human-rights abuses allegedly committed by sovereign states (all but conceding that the injunction interferes with foreign sovereigns, *infra*, p.25), but those are not part of this case. Purported CFAA violations against WhatsApp do not justify an injunction designed to block human

rights abuses for which NSO is not responsible. That task is better left to the "political branches or other international actors." *Cisco*, slip op. 14.

Even WhatsApp recognizes this much. Departing from *Amici*, WhatsApp denies (AB.62-63) that the injunction regulates "encryption policy" or the "development of surveillance technology," claiming it "simply bars NSO from accessing WhatsApp's protected systems, intercepting users' communications, and collecting users' data without authorization." That mischaracterizes the injunction, as outlined *infra*, Part II.D, which bans a wide stripe of legal conduct.

D. The Injunction Is Overbroad

At minimum, the injunction should be vacated because it prohibits lawful conduct (a defect *Amici* ignore), including mere contract breaches, and regulates sovereigns. OB.50-53.

WhatsApp purports to justify the injunction's overbreadth with the truism that injunctions may reach acts "related" to illegal conduct (AB.63). "[T]rue, but injunctive relief should be no more burdensome to the defendant than necessary," *Oracle USA, Inc. v. Rimini St., Inc.*, 81 F.4th 843, 857 (9th Cir. 2023) (cleaned up) (distinguishing *United States v. U.S. Gypsum Co.*, 340 U.S. 76 (1950)). *See* OB.50-51. WhatsApp must show, by "clear and convincing evidence," that banning legal conduct would be "necess[ary]" to prevent "future copyright violations." *Rimini*, 81 F.4th at 857-58 (vacating injunction without deference). Even *Gypsum*, WhatsApp's

main overbreadth case, emphasizes that injunctive provisions banning legal conduct are reviewed more stringently than for mere abuse "of discretion." 340 U.S. at 89. *Contra* AB.63. And *McComb v. Jacksonville Paper Co.*, 336 U.S. 187, 192 (1949) (cited AB.67), only permits injunctions that bar "violations of" statutes, not lawful conduct.

WhatsApp does not dispute that §§ 3(a)-(d) of the injunction—prohibiting the (1) use of any technology that interacts with the WhatsApp app, (2) collection of any data from any phone with a WhatsApp app, (3) reverse-engineering software, and (4) creation of any WhatsApp accounts—bar lawful activity. *See* OB.51-52, 64-66. Creating a WhatsApp account is thus not, as WhatsApp pretends (AB.64), "the same type or class as unlawful acts which the court has found to have been committed" because it is *not* unlawful. *Rimini*, 81 F.4th at 852 (citation omitted). Nor is it inherently tied to illegal activity. And WhatsApp does not even pretend the court found, by clear and convincing evidence, that §§ 3(a)-(d) were *necessary* to prevent future intrusions into WhatsApp's servers. This failure to apply the right legal test is itself an abuse of discretion and grounds for vacatur. *See, e.g.*, *United States v. Ponce*, 22 F.4th 1045, 1046 (9th Cir. 2022).

WhatsApp again tries to defend the court's decision on grounds the court did not endorse. It again fails to persuade.

On §§ 3(a), (c) & (d), WhatsApp says (AB.67) that NSO previously created WhatsApp accounts and reverse-engineered the WhatsApp app to devise its prior exploits, but that is not enough. Someone who illegally downloads music likely purchased a computer before doing so, but an injunction against future piracy should not preclude the purchase of a laptop. *Rimini* thus held that barring de minimis software copying was not justified by a need to ban substantial copying, even though de minimis copying was, of course, part and parcel of substantial copying. 81 F.4th at 857-58. The only operative CFAA/CDAFA theory here had NSO supposedly exceeding authorized access specifically to "the WhatsApp servers." 1-ER-64. That does not justify a ban on using WhatsApp on NSO's own phones.

Nor does WhatsApp respond to NSO's argument that § 3(c), because it purports to ban future breaches of contract terms prohibiting reverse-engineering, also runs afoul of California law categorically barring injunctions against future contract breaches. *See* OB.39 & n.2. WhatsApp's footnoted assertion (AB.49-50 n.8) that NSO "overstates the rule" amounts to no cognizable response at all.

On § 3(b), WhatsApp distracts from the actual issue when it says (AB.65) it is unclear how NSO's "vectors operate."[3] Section 3(b) prevents NSO from

[3] While pushing this irrelevant line, WhatsApp cites *AK Futures*, 35 F.4th at 695, for the proposition that "[a]n injunction need not be drawn around technical lines that the defendant has placed beyond the court's view," (AB.66). *AK Futures* says no such thing.

collecting data from a WhatsApp application on any phone, without regard to WhatsApp servers, even when the NSO user authorizes the access to their phone. Prohibiting NSO from looking at any phone that has installed WhatsApp (i.e., 99% of Israeli phones, and 69% of non-China Internet users[4]), *regardless of whether NSO has permission to do so*, is not "tailored" to CFAA violations (AB.66).

Last, WhatsApp admits (AB.66) the injunction "limit[s] the tools or services *NSO* can provide to its [sovereign] customers," and does not dispute the injunction requires NSO to affirmatively "disable" sovereign' access to its software. That is extraordinary and a blow to law enforcement and intelligence operations around the world. The injunction as written would even prevent NSO from ever providing tools to the *United States*. Just days ago, the Supreme Court held that a suit against an American company accused of aiding and abetting Chinese surveillance risked interfering with U.S. foreign policy. *Cisco*, slip op. 9. At minimum, interfering with sovereigns was contrary to the district court's intentions, 1-ER-21-22, and grounds for remand.

[4] Yinon Ben Shushan, *WhatsApp, YouTube, and Facebook: What are the most popular apps used in Israel in 2025?*, Jerusalem Post (Oct. 6, 2025), https://perma.cc/X2TV-AFZL; "WhatsApp Statistics and Insights [2026]," Armin (May 8, 2026), https://perma.cc/YM5T-A465.

III. WHATSAPP CANNOT DEFEND THE PUNITIVE DAMAGES AWARD

The punitive damages award should be vacated because the district court improperly excluded evidence of NSO's intent, and the award is excessive. WhatsApp fails to refute these charges.

A. NSO's Intent Evidence Was Wrongly Excluded

WhatsApp asserts (AB.68) that the evidentiary ruling below should "receive 'great deference,'" and can be reversed only if "manifestly erroneous" (citations omitted). But "this deferential language is simply another way of saying that [this Court's] review is for abuse of discretion rather than de novo." *Sidibe v. Sutter Health*, 103 F.4th 675, 691 (9th Cir. 2024). WhatsApp also ignores that the district court overlooked that Federal Rule of Evidence 403 "sets a high bar for exclusion." *Id.*; *see* 1-ER-34-40; *see also United States v. Johnson*, 89 F.4th 997, 1002-03, 1003 & n.1 (7th Cir. 2024) (collecting reversals).

WhatsApp then rewrites the court's opinion. It claims (AB.68-69) the court excluded NSO's good-intent evidence on relevance grounds under Rule 401. Not so. The district court ruled based on Rule "403" without mentioning Rule 401. 1-ER-39; *see* 1-ER-35-39. Because Rule 403 exclusion is committed to the trial court's discretion, this Court should not affirm on grounds "the district court did not address." *E.g.*, *United States v. Roldan*, 167 F.4th 569, 578 n.7 (2d Cir. 2026).

WhatsApp's relevance argument also fails. The court invited the jury to award punitive damages if NSO acted with "malice," which hinges on NSO's "intent to cause injury." 2-ER-301; *accord* Cal. Civ. Code § 3294(a), (c)(1). A defendant that designs a tool for lawful purposes and terminates licenses upon misuse is not acting with "intent to injure." *In re V.V.*, 51 Cal. 4th 1020, 1028 (2011) (defining malice). The excluded evidence bore on why *NSO* did what it did: how it designed Pegasus, contracted with clients, and monitored and terminated licenses. 2-ER-311-12. WhatsApp's evidence was equally "untethered from" specific WhatsApp users (AB.69), and focused generally on Pegasus's functionality and how NSO interacted with clients, not any specific intrusion. FER-16-17.

WhatsApp's defense of the court's prejudice theory is equally unpersuasive. It says (AB.68-69) it could not "test whether NSO's screening procedures were followed" because NSO lacked such "knowledge" itself. But WhatsApp did not need to know more than NSO did about its customers to test *NSO's intent*. WhatsApp's real argument—that purported gaps in NSO's knowledge undermine its professions of good faith—remained fully available, including on cross. The jury should have been permitted to weigh both sides' best evidence and decide whether NSO genuinely intended its product for lawful purposes.

Nor can WhatsApp defend the exclusion as a de facto discovery sanction. OB.54-55. It acknowledges (AB.69-70) that sanctions-based exclusion required

finding intentional noncompliance with a discovery order, and that the court never conducted the requisite analysis. The court nonetheless applied a de facto sanction against NSO for not producing certain information due to Israeli export restrictions, without applying Federal Rule of Civil Procedure 37 or undertaking a requisite comity analysis. 1-ER-35-36; *see Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for S. Dist. of Iowa*, 482 U.S. 522, 543-44 (1987).

Finally, the prejudice here was severe and uncured, given WhatsApp's one-sided narrative about NSO's spyware "target[ing]" 1,400 purported "victims." 2-ER-223. By contrast, "[t]he jury heard the law-enforcement theme" (AB.70) only in the sense that NSO said in its opening that "NSO licenses exclusively to government agencies." SER-97. It could not mention the vetting, oversight, and termination procedures that brought gravity and reality to its intent defense. This exclusion did not "cut both ways" (AB.70). WhatsApp conveyed that NSO's actions were wholly unchecked, telling the jury NSO's spying had "global coverage," gave Pegasus users "unlimited access" to "encrypted content," and "uncover[ed] virtual identities." 2-ER-226. In any case, wrongful exclusion under Rule 403 "presume[s] prejudice unless it is more probable than not that the error did not materially affect the verdict," *Sidibe*, 103 F.4th at 691-92 (citation omitted). The jury's initial 376:1 verdict supplies definitive proof of the opposite.

B. The 9:1 Punitives Ratio Violated Due Process

WhatsApp omits this Court's "exacting [de novo] review," and urges (AB.70-71) deference to *nonexistent* factual findings on the three relevant guideposts. *BMW of N. Am., Inc. v. Gore*, 517 U.S. 559, 568 (1996); *see Riley v. Volkswagen Grp. of Am., Inc.*, 51 F.4th 896, 900 (9th Cir. 2022).

Reprehensibility. WhatsApp does not dispute that three of the five reprehensibility factors favor NSO—purely economic harm, no indifference to health or safety, and a plaintiff that is anything but financially vulnerable—or that the court found reprehensibility in equipoise. OB.57. WhatsApp contends (AB.71) that the court—in addressing comparable penalties, not reprehensibility—properly found that NSO engaged in repeated misconduct with ill intent. *See* 1-ER-31. Even if that were right (and it is not clear the court was addressing reprehensibility), the award should not stand.

There was no evidence of "repeated" intrusions by NSO. 1-ER-31. WhatsApp says (AB.72) that "Pegasus was deployed through WhatsApp servers" repeatedly, but it cites no evidence—there is none—that *NSO*, rather than its customers, was responsible for these deployments. *See* 2-ER-118-19; *supra*, Part I.A.3. Pivoting, WhatsApp says (AB.72) that NSO engineered new exploits "three times." That is hardly repeated conduct. And there was no showing that each exploit development violated the CFAA/CDAFA. "The evidentiary record did not show …

specific details about how exactly" NSO developed them. 2-ER-308. Also, Pegasus undisputedly did *not* harm WhatsApp servers. 2-ER-237-38. Last, purported intrusions on third-party phones cannot inflate the award. *Philip Morris USA v. Williams*, 549 U.S. 346, 353 (2007).

WhatsApp cannot cite any findings about "malice and deceit" (AB.72), and "a predicate to any obligation to defer is the existence of findings of fact." *Lompe v. Sunridge Partners, LLC*, 818 F.3d 1041, 1063 (10th Cir. 2016). WhatsApp says (AB.72) this Court can defer to the jury's general verdict. But a jury verdict "setting the amount of the punitive damages is neither a factual finding nor entitled to deference." *Lompe*, 818 F.3d at 1064. WhatsApp's one argument (AB.72)—that NSO "organized its operations to stay hidden" by design—withers under de novo scrutiny. That is at best evidence of a par-for-the-course CFAA/CDAFA violation (*but see* Part I.A), not an egregious one justifying 9x punitive damages.

Proportionality. WhatsApp does not dispute (AB.74) that it was legal error to find the compensatory damages insignificant, and to inflate the award due to WhatsApp's wealth. OB.59-61. WhatsApp argues (AB.74-75) only that a 9:1 ratio is justified based on its reprehensibility arguments. Not so, for three reasons.

First, WhatsApp has no answer to NSO's argument that, under *State Farm Mut. Auto. Ins. Co. v. Campbell*, 538 U.S. 408, 425 (2003), punitive damages should be reduced when compensatory damages are substantial. OB.61.

Second, NSO's conduct was not egregious, as explained *supra*, pp.28-30.

Third, even if WhatsApp were right (AB.75) that reprehensibility factors go "both ways," that requires a lower ratio. *See, e.g.*, *Est. of Hill ex rel. Grube v. NaphCare, Inc.*, 2025 WL 1588738, at *4 (9th Cir. June 5, 2025) (8.7:1 ratio is too high when only two factors were "egregious"); *S. Union Co. v. Irvin*, 563 F.3d 788, 791-92 (9th Cir. 2009) (3:1 ratio "but not more" when "most of the indicia of reprehensibility do not appear"). WhatsApp distinguishes (AB.73 n.11) NSO's other cases based on "case-specific facts," but it misses the point. This Court has repeatedly held that a 4:1 ratio is the ceiling when egregiousness factors are mixed.

Comparable penalties. WhatsApp again fails to defend the district court's reasoning. That *State Farm* did not "dwell long" on comparable civil penalties, 538 U.S. at 428, does not permit, as WhatsApp suggests (AB.75), the court to ignore this factor. *See* OB.62. Nor did *Ramirez v. TransUnion LLC*, 951 F.3d 1008 (9th Cir. 2020), *rev'd on other grounds*, 594 U.S. 413 (2021), or *Hardeman v. Monsanto Co.*, 997 F.3d 941 (9th Cir. 2021), treat this factor as irrelevant (AB.75). *Ramirez* held this factor had no weight when, unlike here, the statute had no "'truly comparable' civil penalty." 951 F.3d at 1037 (citation omitted). And *Hardeman* did not address the factor because the parties "failed" to address it. 997 F.3d at 975. That statutory penalty is especially instructive, given that $1-2 million punitive awards have been deemed excessive relative to $10,000 statutory penalties. *See* OB.61-62. WhatsApp

claims (AB.76) that this penalty is imposed against "trivial" violations. In fact, $10,000 is the penalty for "felony" violations. Cal. Penal Code § 502(d)(1).

WhatsApp proposes another flawed alternative affirmance ground, claiming (AB.76) the award corresponds to $10,000 multiplied by the "tens of thousands" of devices NSO "installed Pegasus on" (citation omitted). But (1) those figures refer to NSO's *customers'* installations, not *NSO*'s, and (2) purported third-party harm cannot inflate punitive damages. *Supra*, Part I.A.3.

CONCLUSION

This Court should reverse the liability determination, vacate (or at least narrow) the permanent injunction, and vacate or remit the punitive damages award.

Dated: July 1, 2026

Respectfully submitted,

/s/ Derek L. Shaffer

STEPHEN A. BROOME
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
865 S. Figueroa St., 10th Floor
Los Angeles, CA 90017
(213) 443-3000
stephenbroome@quinnemanuel.com

HOPE D. SKIBITSKY
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
295 5th Ave., 9th Floor
New York, NY 10016
(212) 849-7000
hopeskibitsky@quinnemanuel.com

DEREK L. SHAFFER
RACHEL FRANK QUINTON
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
555 13th St. NW, Suite 600
Washington, DC 20004
(202) 538-8000
derekshaffer@quinnemanuel.com
rachelquinton@quinnemanuel.com

ALEX H. LOOMIS
QUINN EMANUEL URQUHART
& SULLIVAN, LLP
111 Huntington Ave., Suite 520
Boston, MA 02199
(617) 712-7100
alexloomis@quinnemanuel.com

Counsel for Defendants-Appellants
NSO Group Technologies Limited and Q Cyber Technologies Limited

CERTIFICATE OF COMPLIANCE

Pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C) and Circuit Rule 32-1, the above brief is in 14-point, proportionally spaced Times New Roman type and contains 6,994 words, excluding the items exempted by Fed. R. App. P. 32(f).

Dated: July 1, 2026

/s/ Derek L. Shaffer
Derek L. Shaffer

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the above Reply Brief with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate ACMS system. I certify that all participants in the case are registered ACMS users and that service will be accomplished by the appellate ACMS system.

Dated: July 1, 2026

/s/ Derek L. Shaffer
Derek L. Shaffer