Docket Nos. 24-2179 (L), 24-3463

In the

United States Court of Appeals

For the

Ninth Circuit

CARLOS DADA, et al.,

Plaintiffs-Appellants,

v.

NSO GROUP TECHNOLOGIES LIMITED, et al.,

Defendants-Appellees.

Appeal from a Decision of the United States District Court for the Northern District of California, No. 3:22-cv-07513-JD · Honorable James Donato

EXCERPTS OF RECORD

CAROLINE DECELL
JAMEEL JAFFER
STEPHANIE KRENT
ANNA "MAYZE" TEITLER
NICOLE MO
KNIGHT FIRST AMENDMENT INSTITUTE AT COLUMBIA UNIVERSITY
475 Riverside Drive, Suite 302
New York, New York 10115
Tel: (646) 745-8500
carrie.decell@knightcolumbia.org
jameel.jaffer@knightcolumbia.org
stephanie.krent@knightcolumbia.org
mayze.teitler@knightcolumbia.org
nicole.mo@knightcolumbia.org

COREY STOUGHTON
ALVARO MON CUREÑO
SELENDY GAY PLLC
1290 Avenue of the Americas, 17th Floor
New York, New York 10104
Tel: (212) 390-9000
cstoughton@selendygay.com
amoncureno@selendygay.com

Attorneys for Appellants Carlos Dada, Sergio Arauz, Gabriela Cáceres Gutiérrez, Julia Gavarrete, Roman Gressier, Gabriel Labrador, Ana Beatriz Lazo Escobar, Efren Lemus, Daniel Lizárraga, Carlos López Salamanca, Carlos Martínez, Óscar Martínez, María Luz Nóchez, Víctor Peña, Nelson Rauda Zablah, Daniel Reyes Martínez, Mauricio Sandoval Soriano, and José Luis Sanz

Index

Judgment (ECF No. 79), filed March 8, 2024 ..... ER-003

Order on Motion to Dismiss (ECF No. 78), filed March 8, 2024 ..... ER-004

Declaration of Roy Blecher (ECF No. 46-1), filed April 21, 2023 ..... ER-011

Order Granting Administrative Motion to Relate Case (ECF No. 36), filed January 6, 2023 ..... ER-014

Amended Complaint (ECF No. 31), filed December 16, 2022 ..... ER-015

Exhibit A to Amended Complaint (ECF No. 31-1), filed December 16, 2022..... ER-054

Notice of Appeal (ECF No. 84), filed May 29, 2024 ..... ER-078

Notice of Appeal (ECF No. 80), filed April 8, 2024 ..... ER-081

Docket Report ER-084

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CARLOS DADA, et al.,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED, et al.,

Defendants.

Case No. 3:22-cv-07513-JD

JUDGMENT

Pursuant to the order of dismissal on *forum non conveniens* grounds, Dkt. No. 78, and Federal Rule of Civil Procedure 58, judgment is entered against plaintiffs.

IT IS SO ORDERED.

Dated: March 8, 2024

JAMES DONATO
United States District Judge

United States District Court
Northern District of California

United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

CARLOS DADA, et al.,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED, et al.,

Defendants.

Case No. 3:22-cv-07513-JD

ORDER RE MOTION TO DISMISS

Plaintiffs are "journalists and others who write, produce, and publish El Faro, a digital newspaper based in El Salvador" said to be "one of the foremost sources of independent news in Central America." Dkt. No. 31 ¶ 4. Defendants are NSO Group Technologies Limited and Q Cyber Technologies Limited (together, NSO), which are incorporated and located in Israel. *Id.* ¶¶ 32-33. This case is one of several in this District alleging that NSO supplies "Pegasus" and other software products that allow hackers to "take full control of a target's smartphone remotely and surreptitiously," and thereby obtain access to the target's texts, calls, GPS location, stored data, and other information. *Id.* ¶ 38. NSO is said to have "sold Pegasus to authoritarian and rights-abusing governments" for use against "journalists, human rights activists, and political opponents." *Id.* ¶ 46.

Plaintiffs say they were subjected to "Pegasus attacks" on their devices in 2020 and 2021 as "part of a coordinated and sustained effort to undermine independent journalism in El Salvador." *Id.* ¶ 63; *see also id.* ¶ 53 ("Between June 2020 and November 2021, Defendants and their clients surreptitiously installed Pegasus on the devices of at least thirty-five individuals working in and around El Salvador."). Of the 18 named plaintiffs, 16 allege that the compromised device was "an iPhone 11 owned by El Faro." *See id.* ¶¶ 65, 69, 73, 77, 81, 85, 89, 93, 97, 101,

105, 113, 117, 121, 125, 129. One plaintiff's device was "an iPhone 8 owned by El Faro." *Id.* ¶ 109. The complaint states that virtually all of the attacks occurred in El Salvador in connection with news stories plaintiffs were covering within that country. *See, e.g., id.* ¶¶ 55-59 (alleging hacking incidents while plaintiffs reported in El Salvador on Salvadoran presidential elections and candidates, MS-13 gang issues, the trial of military officers accused of human rights violations, and the like); *see also id.* ¶ 59 & Exh. A (incorporating in complaint a "list of known attacks on individuals in El Salvador, including Plaintiffs and other El Faro employees"). One attack involved a correspondent for El Faro in Washington, D.C. *Id.* ¶ 132.

Plaintiffs sued NSO for violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a), the California Comprehensive Computer Data Access and Fraud Act (CDAFA), California Penal Code § 502(c), and for trespass to chattels, and intrusion upon seclusion. They filed the lawsuit here even though none of the plaintiffs lived or worked within the Northern District of California, *see* Dkt. No. 31 ¶¶ 14-31 (stating most plaintiffs were located in El Salvador, and one in Washington D.C.), and NSO did not have a presence here. The only apparent hook for filing in our District is the allegation "on information and belief" that "some" Apple servers used by defendants to access plaintiffs' iPhones "are located in California," *id.* ¶ 3.

NSO asks to dismiss on a variety of jurisdictional and pleadings challenges under Federal Rules of Civil Procedure 12(b)(2) and 12(b)(6). Dkt. No. 46. The most salient argument is that dismissal is warranted on the basis of *forum non conveniens* because the case involves foreign plaintiffs, foreign defendants, and foreign conduct, and should be decided by a court in Israel or elsewhere. The Court had no trouble rejecting a similar *forum non conveniens* challenge that NSO raised in a case brought by Apple because the facts alleged there amply demonstrated that this District is the best forum for resolving Apple's claims. *See Apple Inc. v. NSO Group Technologies, Inc.*, Case No. 21-cv-09078-JD, 2024 WL 251448, at *1-4 (N.D. Cal. Jan. 23, 2024).

The facts here are very different, and lead to a different result. The Court discussed in detail the doctrine of *forum non conveniens* in *Apple*. In summary, *forum non conveniens* is "a supervening venue provision" that permits the Court to decline jurisdiction when circumstances

indicate that an alternative forum abroad would be a better location for the litigation. *Sinochem Int'l Co. v. Malaysia Int'l Shipping Corp.*, 549 U.S. 422, 429-30 (2007) (internal citation omitted). The Court may dismiss a case under the doctrine "when an alternative forum has jurisdiction to hear [the] case, and . . . trial in the chosen forum would establish . . . oppressiveness and vexation to a defendant . . . out of all proportion to plaintiff's convenience, or . . . the chosen forum [is] inappropriate because of considerations affecting the court's own administrative and legal problems." *Id.* at 429 (quoting *American Dredging Co. v. Miller*, 510 U.S. 443, 447-48 (1994) (quoting in turn *Piper Aircraft v. Reyno*, 454 U.S. 235, 241 (1981) and *Koster v. (American) Lumbermens Mut. Casualty Co.*, 330 U.S. 518, 524 (1947))) (ellipses and alterations in original).

Although a "defendant invoking *forum non conveniens* ordinarily bears a heavy burden in opposing plaintiff's chosen forum," this presumption "'applies with less force'" when, as here, plaintiffs' "choice is not its home forum." *Id.* at 430 (quoting *Piper Aircraft*, 454 U.S. at 255-56); *see also Lueck*, 236 F.3d at 1145 ("a foreign plaintiff's choice of forum merits less deference than that of a plaintiff who resides in the selected forum, and the showing required for dismissal is reduced.") (citing *Gemini Cap. Grp. v. Yap Fishing Corp.*, 150 F.3d 1088, 1091 (9th Cir. 1998)). In such cases, if "'the balance of conveniences suggests that trial in the chosen forum would be unnecessarily burdensome for the defendant or the court, dismissal is proper.'" *Lockman Found. v. Evangelical All. Mission*, 930 F.2d 764, 767 (9th Cir. 1991) (quoting *Piper Aircraft*, 454 U.S. at 255 n.23); *see also Lueck v. Sundstrand Corp.*, 236 F.3d 1137, 1145 (9th Cir. 2001).

"A party moving to dismiss on grounds of *forum non conveniens* must show two things: (1) the existence of an adequate alternative forum, and (2) that the balance of private and public interest factors favor dismissal." *Loya v. Starwood Hotels & Resorts Worldwide, Inc.*, 583 F.3d 656, 664 (9th Cir. 2009) (internal citation omitted). As our circuit has stated, the private interest factors "include (1) relative ease of access to sources of proof; (2) the availability of compulsory process for attendance of hostile witnesses, and cost of obtaining attendance of willing witnesses; (3) possibility of viewing subject premises; (4) all other factors that render trial of the case expeditious and inexpensive." *Id.* (internal citation omitted).

The public interest factors include "(1) administrative difficulties flowing from court

congestion; (2) imposition of jury duty on the people of a community that has no relation to the litigation; (3) local interest in having localized controversies decided at home; (4) the interest in having a diversity case tried in a forum familiar with the law that governs the action; (5) the avoidance of unnecessary problems in the conflict of laws." *Id*. (internal citation omitted); *see also Lueck*, 236 F.3d at 1145-47 (listing similar factors).

Forum non conveniens "is a non-merits ground for dismissal." *Id.* at 432 (internal citation omitted). This means that the Court may grant dismissal while "bypassing questions of subject-matter and personal jurisdiction, when considerations of convenience, fairness, and judicial economy so warrant." *Id*. Application of the doctrine is entrusted to the Court's sound discretion. *American Dredging*, 510 U.S. at 455; *see also Loya*, 583 F.3d at 663-64 (same).

While it is certainly true that dismissal on *forum non conveniens* grounds should "be employed sparingly," *Glob. Commodities Trading Grp. v. Beneficio de Aroz Choloma, S.A.*, 972 F.3d 1101, 1111 (9th Cir. 2020) (internal citation omitted), this case is tailor made for it. The nub of this case is entirely foreign, and concerns the use of software produced in Israel to hack devices owned by a Salvadoran news service and used by journalists in El Salvador. Every incident described in the complaint involved Salvadoran journalists covering Salvadoran news stories while working primarily in El Salvador.

There is little reason under the *forum non conveniens* factors to undertake the burden of litigating this foreign conduct here. NSO states, and plaintiffs do not dispute, that Israel is an adequate alternative forum. Dkt. No. 46 at 7. This is all the more true because NSO expressly states that, "[a]s a citizen of Israel, NSO is amenable to process in Israel." *Id*.; *see Piper Aircraft*, 454 U.S. at 254 n.22 (alternative forum requirement satisfied when defendant is "amendable to process" in the other jurisdiction) (internal quote omitted). Although the parties gave little attention to the courts of El Salvador as an alternative forum, NSO raised the possibility of litigating plaintiffs' claims in Salvadoran courts under Salvadoran law, Dkt. No. 46 at 1, an invitation to which plaintiffs did not respond.

The question then is whether the private and public interest factors weigh in favor of dismissal. Not all private and public interest factors are present in every case, which is the

situation here. The Court will address the factors the parties discussed, along with others that might be relevant.

For the private interest factors, the parties focus almost exclusively on access to proof and witness availability. Overall, this factor weighs in favor of litigating the case in Israel or elsewhere, and not here. To start, neither side was present in, or had any ties to, this District in connection with the allegations in the complaint. NSO was in Israel at all pertinent times, and all of its material witnesses and evidence are located there. NSO represents that it does not hold property or have employees in California. Dkt. No. 46-2 (Shohat Decl.) ¶ 4. As discussed, all of the plaintiffs lived and worked in El Salvador during the period relevant to the complaint, save for one who was located in Washington D.C. Dkt. No. 31 ¶¶ 14 - 31. Plaintiffs did not demonstrate that any significant quantum of witnesses or evidence may be located in this District. Plaintiffs also did not argue against *forum non conveniens* on the basis of the location of Apple's servers or the possibility of needing third-party evidence from Apple, and so those are not factors here. Even if they had, evidence concerning Apple will not be the main battleground between the parties, and should be readily available in electronic or other accessible form. So too for plaintiffs' suggestion that the pendency of other cases against NSO makes keeping this one here "convenient." Dkt. No. 48 at 10. Plaintiffs do not say why that may be so, and to the extent those cases may have relevant discovery, there are efficient ways of getting it short of shoehorning an entirely foreign case into the District.

All of this is in stark contrast to the circumstances in *Apple*. This District is Apple's home forum, where it is headquartered and where its witnesses and evidence are located, and Apple's claims are based on NSO's alleged hacking of Apple's servers and devices located here. *See Apple*, 2024 WL 251448, at *1-2.

Litigating the case in this District would likely impose significantly heavier burdens on NSO than plaintiffs. Israel is more than twice as far away from San Francisco (approximately 7400 air miles) as El Salvador (approximately 2600 air miles), which will disproportionately burden NSO for trial and other court proceedings. This is particularly so because NSO will be the source of substantially more evidence and witnesses than plaintiffs.

The public interest factors also weigh against litigation in this District. Plaintiffs did not demonstrate any local interest or stake in the events alleged in the complaint. Plaintiffs say that California has a "compelling interest in protecting California companies from being used as spyware vectors in violation of state law," Dkt. No. 48 at 9-10, but even accepting that as true for present purposes, California's interest will by amply protected in Apple's lawsuit against NSO, which is now proceeding apace in this Court. Plaintiffs also say that California has a stake in "protecting the ability of El Faro's California readers to access El Faro's reporting," *id.* at 10, but why that might be so is left unsaid. A good argument can be made that California has no interest whatsoever in El Faro's readership. Plaintiffs' suggestion that the case should be litigated here because the United States has an interest in managing the use of spyware is a massive generalization of no utility for the *forum non conveniens* analysis. Almost anything could be justified when painted in such broad strokes. The passing mention of alleged interference with communications between plaintiffs and U.S. embassy officials does not compel a different conclusion.

Burdening a jury in this District with all of this makes little sense. Time and again, the Court has been awed by the conscientiousness of jurors in this District, who we ask to drop everything on a moment's notice to decide civil and criminal cases of often great complexity. Even so, a local jury would understandably struggle with being asked to sit for a long trial that involves purely foreign plaintiffs and defendants, and events in foreign lands.

That is basically all the parties say about *forum non conveniens*. The Court adds that plaintiffs did not explain why a trial here would be more expeditious and inexpensive than in Israel or elsewhere. It may be that the Court has greater familiarity with the federal and state laws featured in the complaint, but that is merely because plaintiffs chose to invoke the laws of this forum. Plaintiffs did not suggest that they would not have plausible claims under the laws of other forums, with concomitant judicial expertise there. The possibility that they may not be able to allege claims under federal or California state law is of little moment. *See Piper Aircraft*, 454 U.S. at 247 ("[t]he possibility of a change in substantive law should ordinarily not be given conclusive or even substantial weight in the *forum non conveniens* inquiry.").

Overall, this case could not be more different than *Apple* for *forum non conveniens* purposes. It belongs in a court in Israel or El Salvador, and not here. Fairness, convenience, and judicial economy demand no less. To conclude otherwise would open the doors of the federal courts to lawsuits by foreign entities for conduct that occurred entirely outside the United States, a result that cannot be squared with our traditional understanding of due process and limited jurisdiction.

Nothing in the record indicates that plaintiffs could amend the complaint in ways that might overcome the application of *forum non conveniens* here. Plaintiffs did not ask to amend. The Court need not reach the personal jurisdiction or other arguments for dismissal raised by NSO. *See Sinochem*, 549 U.S. at 429 ("forum non conveniens may justify dismissal of an action though jurisdictional issues remain unresolved").[1] Consequently, the case is dismissed and ordered closed.

IT IS SO ORDERED.

Dated: March 8, 2024



JAMES DONATO
United States District Judge

[1] The Court granted leave to file an amicus brief to a group of "legal scholars." Dkt. No. 55. The brief addressed only personal jurisdiction over NSO in this District. *See* Dkt. No. 51-1 at 1. Because the Court need not reach that issue, the amicus brief is effectively moot.

JOSEPH N. AKROTIRIANAKIS (Bar No. 197971)
jakro@kslaw.com
AARON S. CRAIG (Bar No. 204741)
acraig@kslaw.com
KING & SPALDING LLP
633 West Fifth Street, Suite 1700
Los Angeles, CA 90071
Telephone: (213) 443-4355
Facsimile: (213) 443-4310
Attorneys for Defendants NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CARLOS DADA, *et al.*,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LTD. and Q CYBER TECHNOLOGIES LTD.

Defendants.

Case No. 3:22-cv-07513-JD
[*Honorable James Donato*]

DECLARATION OF ROY BLECHER IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS

Date: May 25, 2023
Time: 10:00 a.m.
Ctrm: 11

I, Roy Blecher, declare as follows:

1. I am an attorney licensed to practice law in Israel, and I am a partner and co-founder of the law firm of Krispin, Rubinstein, Blecher, Kadouch & Partners. I represent Defendants NSO Group Technologies Ltd. and Q Cyber Technologies Ltd. ("Defendants") in connection with this matter, and I have represented Defendants in a number of other matters in Israel. I have personal knowledge of the facts set forth below and, except as otherwise stated, could testify competently to each fact averred herein.

2. I have 28 years of experience as a licensed attorney handling civil and criminal matters in Israel, including having participated in hundreds of trials. In civil and criminal matters in Israel there are no pretrial depositions or any other alternative means to examine a witness under oath prior to trial. I have heard of instances of Israeli witnesses being compelled, pursuant to the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, to testify under oath in a deposition in American civil proceedings, but such proceedings are very rare.

3. I have reviewed the complaint in this lawsuit. Based on my review of the plaintiff's allegations, it would appear that any testimony from a current or former NSO employee located in Israel would likely involve questions, the answers to which would implicate Israel's Defense Export Control Law ("DECL") and other Israeli laws pertinent to the sensitive activities of NSO. A witness' answering such questions might violate Israeli law and carry criminal penalties.

4. Israeli law includes a privilege against self-incrimination. Moreover, a witness testifying before an Israeli court would have the right not to give testimony that would constitute a criminal offense under Israeli law. In my experience, if a question is asked in an Israeli court and answering the question could incriminate the witness, the witness or the witness' attorney will object and assert the witness' privilege against self-incrimination. In those circumstances, if the presiding judge orders the witness to answer the question, the witness' testimony cannot be used as evidence against him in any subsequent criminal proceeding.

5. Additionally, based on my experience practicing law in Israel, I believe that agreements may be able to be reached with the Israeli government that, together with procedures available under Israeli law (such as in camera hearings, gag orders, and security clearances for counsel in the matter), could be implemented to enable a witness who is willing to testify to do so without fear of prosecution. I do not believe the Israeli government would be willing to make such agreements concerning testimony to be given in a deposition for use in a foreign court.

6. Based on the forgoing, I do not believe that any party to an American proceeding could effectively take the testimony of an Israeli witness, in Israel, if the witness' testimony would include answers about technology and other sensitive information that is subject to the DECL and other Israeli laws, and which if given would constitute criminal offenses under Israeli law.

I declare under the penalty of perjury and the laws of the United States that the foregoing is true and correct this 9th day of March 2023, at Bnei Brak, Israel.



ROY BLECHER

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

RELATED CASE ORDER

A Motion for Administrative Relief to Consider Whether Cases Should Be Related or a *Sua Sponte* Judicial Referral for Purpose of Determining Relationship (Civil L.R. 3-12) has been filed. The time for filing an opposition or statement of support has passed. As the judge assigned to case:

3:21-cv-09078-JD
Apple Inc. v. NSO Group Technologies Limited

I find that the more recently filed case(s) that I have initialed below are related to the case assigned to me, and such case(s) shall be reassigned to me. Any cases listed below that are not related to the case assigned to me are referred to the judge assigned to the next-earliest filed case for a related case determination.

Case	Title	Related	Not Related
22-cv-07513-WHA	Dada v. NSO Group Technologies Limited	**JD**	

ORDER

The parties are instructed that all future filings in any reassigned case are to bear the initials of the newly assigned judge immediately after the case number. Any case management conference in any reassigned case will be rescheduled by the Court. The parties shall adjust the dates for the conference, disclosures and report required by Fed. R. Civ. P 16 and 26 accordingly. Unless otherwise ordered, any dates for hearing noticed motions are vacated and must be re-noticed by the moving party before the newly assigned judge; any deadlines set by the ADR Local Rules remain in effect; and any deadlines established in a case management order continue to govern, except dates for appearance in court, which will be rescheduled by the newly assigned judge.

Dated: January 5, 2023

By: _____
JAMES DONATO
United States District Judge

PAUL HOFFMAN #71244
JOHN WASHINGTON #315991
Schonbrun, Seplow, Harris,
Hoffman & Zeldes LLP
200 Pier Avenue, Suite 226
Hermosa Beach, CA 90254
T: (424) 297-0114
F: (310) 399-7040
hoffpaul@aol.com

*Counsel for all Plaintiffs**

**See Signature Page for Complete List of Plaintiffs*

CARRIE DECELL, *Pro Hac Vice*
JAMEEL JAFFER, *Pro Hac Vice*
ALEX ABDO, *Pro Hac Vice*
STEPHANIE KRENT, *Pro Hac Vice*
EVAN WELBER FALCÓN, *Pro Hac Vice*
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
T: (646) 745-8500
F: (646) 661-3361
carrie.decell@knightcolumbia.org

*Counsel for all Plaintiffs**

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

CARLOS DADA, SERGIO ARAUZ, GABRIELA CÁCERES GUTIÉRREZ, JULIA GAVARRETE, ROMAN GRESSIER, GABRIEL LABRADOR, ANA BEATRIZ LAZO ESCOBAR, EFREN LEMUS, DANIEL LIZÁRRAGA, CARLOS LÓPEZ SALAMANCA, CARLOS MARTÍNEZ, ÓSCAR MARTÍNEZ, MARÍA LUZ NÓCHEZ, VÍCTOR PEÑA, NELSON RAUDA ZABLAH, DANIEL REYES MARTÍNEZ, MAURICIO SANDOVAL SORIANO, and JOSÉ LUIS SANZ,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No. 3:22-cv-07513-WHA

AMENDED COMPLAINT

DEMAND FOR JURY TRIAL

INTRODUCTION

1. Defendants NSO Group Technologies Limited and Q Cyber Technologies Limited develop spyware—malicious surveillance software—and sell it to rights-abusing governments. With Defendants' technology and assistance, these governments surveil journalists, human rights advocates, and political opponents, often in the service of broader campaigns of political intimidation and persecution. As the U.S. Department of Commerce observed last year when it added NSO Group to its "Entity List," Defendants' spyware has enabled authoritarian governments to "conduct transnational repression"—to reach across borders and stifle dissent. In recent years, the supply of spyware to authoritarian and other rights-abusing governments, by Defendants and other mercenary spyware companies, has become a grave and urgent threat to human rights and press freedom around the world.

2. Defendants' signature product, usually sold under the name "Pegasus," is a particularly sophisticated and insidious type of spyware. Defendants and their clients can install Pegasus on a target's smartphone remotely and surreptitiously, without any action by the target. Once installed, Pegasus gives its operators essentially full control of the device. They can covertly extract contact lists, calendar entries, text and instant messages, notes, emails, search histories, and GPS locations. They can turn on the smartphone's microphone to record surrounding sounds. They can activate the smartphone's camera to take photographs. They can also copy authentication keys to gain access to cloud-based accounts. Defendants highlight these and other capabilities in their marketing materials.

3. Defendants developed Pegasus, and deploy it, by repeatedly accessing computer servers owned by U.S. technology companies, including Apple Inc., a company based in Cupertino, California. As relevant to this case, Defendants accessed Apple servers to identify and exploit vulnerabilities in Apple software and services, to enable the delivery of Pegasus to targets' iPhones, and to allow Pegasus operators to extract data from their targets' iPhones and their targets' cloud-based accounts. On information and belief, some of the Apple servers that Defendants abused to facilitate the delivery and operation of Pegasus in this case are located in California. In November 2021, Apple sued Defendants in this district, asserting that, through their development

and deployment of spyware, they had exploited Apple's software and services, damaged its business and goodwill, and injured its users.

4. Plaintiffs in this case include journalists and others who write, produce, and publish El Faro, a digital newspaper based in El Salvador that has become one of the foremost sources of independent news in Central America—in the words of the International Press Institute, a "paragon of investigative journalism . . . with its fearless coverage of violence, corruption, inequality, and human rights violations." El Faro has a broad readership not only in Central America, but also in the United States, and particularly here in California. Plaintiffs include Carlos Dada, El Faro's co-founder and director; Roman Gressier, an El Faro reporter who is a U.S. citizen; Nelson Rauda Zablah, a former El Faro reporter who currently lives in the United States; José Luis Sanz, the Washington correspondent for El Faro, who also currently lives in the United States; and fourteen other El Faro employees.

5. Between June 2020 and November 2021, at least twenty-two people associated with El Faro, including Plaintiffs, were the victims of Pegasus attacks. Their devices were accessed remotely and surreptitiously, their communications and activities monitored, and their personal data accessed and stolen. Many of these attacks occurred when they were communicating with confidential sources, including U.S. Embassy officials, and reporting on abuses by the Salvadoran government. The journalists and others who were the victims of these Pegasus attacks learned of them only much later. When they came to light, the attacks were condemned by human rights and press freedom groups around the world. For example, a coalition of civil society groups from Central America and the United States issued a joint statement in January 2022 denouncing the attacks and decrying "[t]he lack of accountability for such egregious conduct by public authorities and private companies."

6. The Pegasus attacks have profoundly disrupted Plaintiffs' lives and work. The attacks have compromised Plaintiffs' safety as well as the safety of their colleagues, sources, and family members. The attacks have deterred some sources from sharing information with Plaintiffs. Some Plaintiffs have been diverted from pressing investigative projects by the necessity of assessing which data was stolen, and of taking precautions against the possibility that the stolen

data will be exploited. Plaintiffs have also had to expend substantial resources to protect their devices against possible future attacks, to ensure their personal safety, and to address serious physical and mental health issues resulting from the attacks. The attacks have undermined the security that is a precondition for the independent journalism that El Faro strives to provide its readers, as well as the ability of El Faro's readers, including those in the United States, to obtain independent analysis of events in Central America.

7. Defendants' development and deployment of Pegasus against Plaintiffs was unlawful. It violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502, and it constituted trespass to chattels and intrusion upon seclusion. This is a suit for injunctive and declaratory relief, as well as compensatory and punitive damages.

JURISDICTION AND VENUE

8. This Court has jurisdiction over Plaintiffs' federal causes of action pursuant to 28 U.S.C. § 1331.

9. This Court has jurisdiction over Plaintiffs' state law causes of action pursuant to 28 U.S.C. § 1367, because these claims arise out of the same nucleus of operative fact as Plaintiffs' federal statutory claims.

10. This Court has personal jurisdiction over Defendants because Defendants have purposefully availed themselves of California as a forum and have purposefully directed their tortious activities at California. A court in this district exercised personal jurisdiction over Defendants based on substantially similar facts in *WhatsApp Inc. v. NSO Group Technologies Limited*, 472 F. Supp. 3d 649 (N.D. Cal. 2020).

11. Alternatively, this Court has personal jurisdiction over Defendants pursuant to Federal Rule of Civil Procedure 4(k)(2), because Plaintiffs' claims arise under federal law; if Defendants are not subject to jurisdiction in California, then they are not subject to jurisdiction in any state's courts of general jurisdiction; and exercising jurisdiction over Defendants is consistent with U.S. law and the U.S. Constitution.

12. Venue is proper in this district pursuant to 28 U.S.C. § 1391(b)(2) or, alternatively, 28 U.S.C. § 1391(b)(3).

DIVISIONAL ASSIGNMENT

13. Pursuant to Civil Local Rule 3-2(e), this case may be assigned to the San Jose division because a substantial part of the events giving rise to Plaintiffs' claims occurred in Santa Clara County, where Apple is located.

PARTIES

Plaintiffs

14. Plaintiff Carlos Dada is the director of El Faro, which he co-founded in 1998. His reporting focuses on corruption and violence, and he has reported from numerous conflict zones, including in Guatemala, Honduras, Iraq, Mexico, and Venezuela. In 2011, he won the Maria Moors Cabot Prize for Latin American Reporting. In 2022, he was honored by the International Press Institute and International Media Support with a World Press Freedom Hero award, which recognizes "journalists who have made significant contributions to promote press freedom, particularly in the face of great personal risk." He also won the 2022 International Center for Journalists' Knight Trailblazer Award for "his hard-hitting investigative reporting, lyrical writing and visionary leadership." He lives in San Salvador, El Salvador.

15. Plaintiff Sergio Arauz is the deputy editor-in-chief of El Faro, where he has worked since 2001. His reporting focuses on politics and human rights. He lives in San Salvador.

16. Plaintiff Gabriela Cáceres Gutiérrez is a reporter for El Faro, where she has worked since 2018. In 2021, she, along with Plaintiffs Carlos Martínez and Óscar Martínez, undertook one of El Faro's most significant investigations, revealing secret negotiations held in maximum security prisons between the Bukele Administration and incarcerated members of El Salvador's three main gangs: Mara Salvatrucha ("MS-13"), Barrio 18 Revolucionarios, and Barrio 18 Sureños. She lives in San Salvador.

17. Plaintiff Julia Gavarrete is a reporter for El Faro, where she has worked since 2021. She has more than a decade of experience reporting in El Salvador and Central America, and her reporting focuses on vulnerable communities in Central America, on women's rights, and on

environmental issues. She currently lives in Berlin, Germany while on a four-month fellowship with Reporters Sans Frontières.

18. Plaintiff Roman Gressier is a reporter for El Faro, where he has worked since November 2019. He writes El Faro's English-language newsletter and has reported extensively on Central American politics, human rights, and press freedom. He is a dual citizen of the United States and France.

19. Plaintiff Gabriel Labrador is a reporter for El Faro, where he has worked since 2011. He has been a reporter for more than eighteen years, and he has reported extensively on criminal justice and public corruption, including on a Salvadoran Supreme Court magistrate's ties to the MS-13 gang, on the political and policymaking roles of President Bukele's brothers, and on detentions during El Salvador's recent "state of exception." He lives in San Salvador.

20. Plaintiff Ana Beatriz Lazo Escobar is a marketing manager for El Faro, where she has worked since 2015. She lives in Tamanique, El Salvador.

21. Plaintiff Efren Lemus is a reporter for El Faro, where he has worked since 2011. He has written about gang violence and El Salvador's attempts to curtail it, about the treatment of detainees during El Salvador's state of exception, and about accusations of wrongdoing and corruption within the governing Nuevas Ideas party. He also co-wrote an in-depth profile of the MS-13 gang for The New York Times. He lives in San Salvador.

22. Plaintiff Daniel Lizárraga currently works for the Institute for War and Peace Reporting as the coordinator for investigative journalism projects in Latin America and Cuba. Mr. Lizárraga previously worked for El Faro, where he served as the investigations editor from January to August 2021. His reporting focuses on corruption, and his work has been recognized with a Gabriel García Márquez Award from the New Journalism Foundation and a Mexican National Journalism Award. He lives in Mexico City, Mexico.

23. Plaintiff Carlos López Salamanca is the general manager of El Faro, where he has worked for four years. He lives in San Salvador.

24. Plaintiff Carlos Martínez is a reporter for El Faro, where he has worked since 2004. He is one of the founding members of Sala Negra, El Faro's investigative journalism team. His

reporting focuses on gang violence and official misconduct. He has worked on some of El Faro's most important stories, including an investigation into the Bukele Administration's secret negotiations with incarcerated gang members, and he co-wrote an in-depth profile of the MS-13 gang for The New York Times. He lives in La Libertad, El Salvador.

25. Plaintiff Óscar Martínez is the editor-in-chief of El Faro, where he has worked since January 2007. A founding member of Sala Negra, he reports on issues of gang violence, migration, and official misconduct. He has been awarded the Fernando Benítez National Journalism Award in Mexico, the José Simeón Cañas Central American University in El Salvador Human Rights Prize, and the Maria Moors Cabot Prize. He lives in San Salvador.

26. Plaintiff María Luz Nóchez is a reporter and the Opinion editor for El Faro, where she has worked since 2011. She reports on arts and culture, violence against women and the LGBTQ community, and the rights of Indigenous people. She lives in Santa Tecla, El Salvador.

27. Plaintiff Víctor Peña is a photojournalist for El Faro, where he has worked since 2016. He contributes photography and other audiovisual and graphic material to El Faro, focusing on issues relating to women's rights, inequality, pollution, and migration. He lives in San Salvador.

28. Plaintiff Nelson Rauda Zablah worked as a reporter and hosted a twice-weekly radio show for El Faro from 2015 to August 2022. He has a decade of experience covering corruption, crime, the justice system, politics, migration, and human rights. His work has also been published in The New York Times, The Washington Post, the Los Angeles Times, ProPublica, the BBC, and El Diario. He previously served as secretary to the Board of Directors of the Asociación de Periodistas de El Salvador, the Salvadoran journalists' association. He currently lives in New York City while pursuing a master's degree at Columbia Journalism School.

29. Plaintiff Daniel Reyes Martínez is the chief technology officer of El Faro, where he has worked for six years. He lives in Antiguo Cuscatlán, El Salvador.

30. Plaintiff Mauricio Ernesto Sandoval Soriano is the general administrator of El Faro, where he has worked since 2018. He lives in Antiguo Cuscatlán.

31. Plaintiff José Luis Sanz is the Washington correspondent for El Faro, where he has worked since 2001. He was the director of El Faro from 2014 to December 2020. A founding

member of Sala Negra, he previously reported on issues of violence, gangs, and organized crime in Central America. He now reports on human rights, migration, and corruption. He currently lives in Washington, D.C.

Defendants

32. Defendant NSO Group Technologies Limited is a limited liability company that was incorporated in Israel on January 25, 2010. NSO Group develops highly sophisticated spyware; sells that spyware to government clients around the world, including to governments associated with grave abuses of human rights; trains those clients in the use of the spyware; and assists those clients in its deployment. NSO Group is a subsidiary of Q Cyber Technologies Limited, and, on information and belief, it sometimes operates under that name.

33. Defendant Q Cyber Technologies Limited is a limited liability company. It was originally incorporated in Israel on December 2, 2013 under the name L.E.G.D. Company Limited, but changed its name to Q Cyber Technologies on May 29, 2016. Q Cyber is the parent company of NSO Group and a subsidiary of OSY Technologies SARL.

34. As discussed further below, Defendants have purposefully directed their tortious activities at the State of California. They have also purposefully availed themselves of the United States, and the State of California in particular. For example, for most of the past decade, NSO Group has been principally funded and controlled by California-based companies, including Francisco Partners and Berkeley Research Group. In addition, Q Cyber established a U.S. sales arm called Westbridge Technologies, Inc. to market Defendants' spyware to law enforcement agencies across the United States. Omri Lavie, one of the three co-founders of NSO Group, co-founded and served as the CEO of Westbridge. Defendants and Westbridge hired U.S.-based firms to help market Defendants' spyware and oversee their public relations in the United States. Defendants and Westbridge endeavored to sell Defendants' technology to U.S. government agencies, including the Central Intelligence Agency, the Drug Enforcement Administration, and the Secret Service, as well as to local law enforcement agencies, including the Los Angeles and San Diego Police Departments. In 2019, Defendants sold a version of Pegasus to the Federal

Bureau of Investigation and trained FBI agents as they tested and evaluated the spyware. The FBI ultimately paid Defendants roughly $5 million in fees.

35. On information and belief, at all times material to this case, each Defendant was the agent, partner, alter ego, subsidiary, parent, and/or co-conspirator of and with the other Defendant, and the acts of each Defendant were within the scope of that relationship; each Defendant knowingly and intentionally agreed with the other to carry out the acts alleged in this Complaint; and in carrying out the acts alleged in this Complaint, each Defendant acted with the knowledge, permission, and consent of the other, and each Defendant aided and abetted the other.

FACTUAL ALLEGATIONS

Pegasus

36. Defendants develop highly sophisticated spyware; sell that spyware to government clients around the world, including to governments associated with grave abuses of human rights; train those clients in the use of the spyware; and assist those clients in its deployment.

37. Defendants' signature product is called Pegasus. Plaintiffs use the term "Pegasus" throughout this Complaint to refer to any of the products that Defendants market that are identical or substantially similar to Pegasus.

38. Pegasus enables its operators to take full control of a target's smartphone remotely and surreptitiously. According to Defendants' marketing materials, Pegasus can be used to remotely and covertly surveil and extract contact details, text messages, instant messages, notes, emails, web-browsing activity, files, and passwords. It can be used to monitor phone calls and VoIP calls, as well as user activity on different applications, including WhatsApp, Facebook, and Skype. It can be used to track and log a device's GPS location. And it can be used to activate the device's microphone to record surrounding sounds, and to activate the device's camera to take photographs.

39. Pegasus can also give its operators access to data stored in the cloud. According to news reports, Pegasus allows its operators to copy the authentication keys that smartphones use to access U.S.-based cloud services such as iCloud, Google Drive, and Facebook Messenger. Pegasus

operators can use those keys to gain access to data stored on those cloud servers—including documents and photographs—without the knowledge of the smartphone's user.

40. It is practically impossible for individuals to protect themselves against Pegasus attacks. Pegasus can be installed surreptitiously, without the smartphone user's involvement or awareness, through "zero-click" attacks. It can be installed remotely, eliminating the need for physical proximity to a target's smartphone as well as any reliance on local mobile network operators. It can also circumvent ordinary security measures—such as the use of encryption—because it allows its operators to access an infected device as though they were the device's user. In addition, it is designed to subvert safeguards that would otherwise alert the target to its presence. On iPhones, for example, Pegasus disables crash reporting to Apple, and many of the malicious processes that Pegasus runs on a device following an infection have been given names similar to those of legitimate iOS system processes.

41. Independent security researchers at the Citizen Lab at the University of Toronto's Munk School of Global Affairs & Public Policy—an organization that has conducted in-depth investigations of spyware attacks around the world—have concluded that Plaintiffs in this case were targeted through zero-click Pegasus attacks directed at their iPhones. Amnesty International's Security Lab independently confirmed the Citizen Lab's conclusion. Investigations by the Citizen Lab's researchers indicate that Defendants carried out these attacks in the stages described below. On information and belief, the Pegasus attacks against Plaintiffs required Defendants to interact extensively with Apple's U.S.-based servers, many of which are in California.

42. First, Defendants identified vulnerabilities in Apple software and services that could be used in the process of infecting targeted iPhones with Pegasus. Defendants created Apple ID accounts specifically for the purpose of identifying these vulnerabilities. Ordinarily, Apple ID accounts are used by Apple to authenticate its customers when they use Apple services. In contrast, Defendants used their Apple ID accounts to discover vulnerabilities in Apple's software, to probe Apple's servers and services, and to test the software that Defendants developed to infect iPhones with Pegasus.

43. Second, Defendants and their clients exploited the vulnerabilities that they identified to infect targeted iPhones with Pegasus. To initiate a zero-click attack, Defendants and their clients used the target's Apple ID or other information to confirm that the target was in fact using an iPhone, and then they used Defendants' own Apple ID accounts to send malicious data to the device by leveraging the communications between Apple's services and the targeted iPhone. The malicious data caused the device to retrieve Pegasus (and other malicious data precipitating the Pegasus infection) through a network of servers operated and/or maintained by Defendants. In this case, Plaintiffs' iPhones were infected using zero-click exploits known as KISMET and FORCEDENTRY. Defendants and their clients appear to have executed both of these exploits by using Apple ID accounts to send malicious data through Apple's iMessage service. In the case of at least FORCEDENTRY, the Pegasus file was stored temporarily, in encrypted form, on one of Apple's iCloud servers before delivery to a target's iPhone.

44. Third, Pegasus operators used command-and-control servers to exploit the Pegasus infection, taking control of the infected iPhone. The operators could use these servers to issue commands to each infected device—for example, to exfiltrate data, to enable location tracking, or to record audio and take photographs using the device's microphone and camera. If a Pegasus operator extracted authentication keys from an infected iPhone, the operator could use those keys to access and extract data from the targeted individual's cloud-based accounts. Pegasus infections were sometimes short-lived (allowing operators to hack their targets' iPhones, exfiltrate data of potential interest, and then attempt to cover their tracks by deleting traces of the infection) and sometimes prolonged or "active" (allowing operators to conduct ongoing surveillance, albeit at greater risk of discovery). Even when Defendants' employees were not themselves the Pegasus operators at this stage of the attacks, Defendants remained involved by configuring and maintaining the operators' command-and-control servers, ensuring that infected devices were running the latest version of the Pegasus software, and providing ongoing technical assistance to the operators. Defendants also offered extensive customer support, including on-the-ground support during the initial deployment and/or continued operation of Pegasus, technical support by

email and phone, and engineer support through remote desktop software and/or a virtual private network.

45. In July 2021, Amnesty International's Security Lab concluded that Defendants were, at that time, able to remotely and covertly compromise all recent iPhone models and versions of Apple's mobile operating system using the process described above or one similar to it.

The Threat Pegasus Poses to Press Freedom and Human Rights

46. Defendants have sold Pegasus to authoritarian and rights-abusing governments around the world, and many of those governments have used the spyware to target journalists, human rights activists, and political opponents.

47. According to the Pegasus Project, a collaboration of more than eighty journalists from seventeen media organizations in ten countries, at least 180 journalists from twenty countries have been selected as targets of Pegasus attacks by authoritarian or rights-abusing governments. Saudi authorities used Pegasus to surveil family members and close associates of journalist Jamal Khashoggi—whom Saudi agents brutally murdered in 2018—as well as other Saudi activists, an Amnesty International staff member, and an American New York Times journalist who has reported extensively on the country. Morocco used Pegasus to spy on journalist Omar Radi. Mexican officials used Pegasus to surveil journalists and lawyers investigating corruption and human rights abuses in the country. Hungarian Prime Minister Viktor Orbán also used Pegasus to surveil journalists, lawyers, and social activists.

48. Prominent human rights activists, diplomats, and political opposition figures, too, have been frequent victims of Pegasus attacks. For example, in 2021 alone, Defendants' clients used Pegasus to surveil U.S. diplomats working in Uganda; Carine Kanimba, a dual U.S.–Belgian citizen who was targeted while she was campaigning for the release of her father, Hotel Rwanda hero Paul Rusesabagina, from detention; Lama Fakih, a prominent Lebanese activist and Human Rights Watch director; at least four members of the civic youth movement "Oyan, Qazaqstan" ("Wake Up, Khazakhstan"); and at least thirty pro-democracy protesters and activists in Thailand. In 2020, more than sixty pro-Catalonian independence activists were the victims of Pegasus attacks. And in 2019, at least three human rights activists in India were surveilled with Pegasus

while they were advocating for the release of other imprisoned activists, and Polish senator Krzysztof Brejza was surveilled with Pegasus while he was running a parliamentary election campaign.

49. The supply of spyware to authoritarian and rights-abusing regimes, by Defendants and other mercenary spyware manufacturers like them, is now widely understood to present an urgent challenge to press freedom around the world.

50. In November 2021, the U.S. Department of Commerce added NSO Group to its "Entity List" based on evidence that it had "supplied spyware to foreign governments that used" the spyware "to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers," as well as to target "dissidents, journalists and activists outside of their sovereign borders to silence dissent." The Commerce Department described the designation of NSO Group as part of a broader effort to "stem the proliferation of digital tools used for repression" and to "improv[e] citizens' digital security, combat[] cyber threats, and mitigat[e] unlawful surveillance." In June 2022, the Biden Administration opposed U.S. government contractor L3Harris Technologies' bid to acquire NSO Group, observing that Pegasus had been "misused around the world to enable human rights abuses, including to target journalists, human rights activists, or others perceived as dissidents and critics." And in its October 2022 National Security Strategy, the Biden Administration pledged "to counter the exploitation of American's [sic] sensitive data and illegitimate use of technology, including commercial spyware and surveillance technology," and to "stand against digital authoritarianism."

51. Congress has also begun to act against the threats posed by spyware. On July 27, 2022, the Chair of the U.S. House Permanent Select Committee on Intelligence called the widespread availability of spyware like Pegasus a "game-changer for autocratic regimes that are looking for new means to surveil, intimidate, imprison, or even kill dissidents, journalists, and others who they view as a threat." The Committee subsequently approved legislation that would empower the Director of National Intelligence to prohibit the U.S. intelligence community from buying and using foreign spyware, and that would authorize the President to impose sanctions on foreign firms and individuals that sell, purchase, or use spyware.

52. Digital security researchers and human rights advocates have also expressed increasing alarm about the implications of spyware for privacy, free speech, and other human rights. Ronald Deibert, Director of the Citizen Lab, has warned that "[a]dvanced spyware is to surveillance [what] nuclear technology is to weapons—it represents a quantum leap forward in sophistication and power." David Kaye, former UN Special Rapporteur on freedom of expression and opinion, has explained that "spyware with the characteristics of Pegasus—the capability to access one's entire device and data connected to it, without discrimination, and without constraint—*already* violates . . . international human rights law," concluding that "[n]o government should have such a tool, and no private company should be able to sell such a tool to governments or others." Dr. Agnès Callamard, Secretary General of Amnesty International and former UN Special Rapporteur on extrajudicial, summary or arbitrary executions, has explained that "[w]e are witnessing a global spyware crisis in which activists, journalists and lawyers are targeted with invasive surveillance as a means to silence and intimidate them."

The Pegasus Attacks on El Faro

53. Between June 2020 and November 2021, Defendants and their clients surreptitiously installed Pegasus on the devices of at least thirty-five individuals working in and around El Salvador. These Pegasus attacks targeted independent journalists and media organizations, as well as leaders of prominent civil society organizations.

54. No organization was more profoundly impacted by the Pegasus attacks than El Faro. A digital newspaper based in El Salvador, El Faro is one of the foremost sources of independent journalism in Central America. It is dedicated to investigative and in-depth reporting on issues including corruption, violence, organized crime, migration, inequality, and human rights. Since its founding in 1998, it has become a regional benchmark for independent, transparent, and reliable journalism. Defendants and their clients subjected at least twenty-two of El Faro's thirty-five employees to repeated Pegasus attacks. These attacks went undetected at first, but subsequent analyses identified 226 Pegasus infections between June 2020 and November 2021 on devices used by El Faro employees. The attacks—which intensified around El Faro's publication of major

stories—damaged devices used by employees for both professional and personal purposes and resulted in the exfiltration of sensitive data.

55. For example, beginning in or around June 2020, Defendants and their clients hacked the device of Plaintiff Carlos Martínez, an El Faro reporter, at least twenty-eight times. The Citizen Lab was able to detect an additional, unsuccessful attempted hack of Mr. Martínez's device using Defendants' FORCEDENTRY exploit on November 15, 2021. During this time, Mr. Martínez was the lead El Faro reporter investigating the secret negotiations between the Salvadoran government and the MS-13 gang.

56. Between September and November 2020, as El Faro first reported on the MS-13 negotiations, Defendants and their clients hacked the devices of El Faro's employees more than two dozen times. Those whose devices were infected with Pegasus during this time include Plaintiffs Carlos Dada, Sergio Arauz, Gabriel Labrador, Carlos López Salamanca, Carlos Martínez, Óscar Martínez, Daniel Reyes Martínez, Mauricio Sandoval Soriano, and José Luis Sanz.

57. Defendants and their clients continued to hack El Faro employees' devices throughout the end of 2020 and beginning of 2021, most frequently targeting Carlos Dada, Carlos Martínez, Óscar Martínez, and José Luis Sanz.

58. The Pegasus attacks increased in intensity. In April and May 2021, Defendants and their clients hacked the devices of El Faro employees fifty-two times. They installed Pegasus on the device of Plaintiff Efren Lemus as he reported that El Salvador's former Minister of Security and Justice had been fired in part because he attempted to mount his own presidential candidacy without President Bukele's support. At the same time, Defendants and their clients hacked the device of Gabriel Labrador while he was conducting interviews for a magazine profile of President Bukele, and they hacked the device Plaintiff Nelson Rauda Zablah while he was covering the trial of sixteen military officers accused of leading the December 1981 massacre of more than one thousand civilians in the village of El Mozote.

59. Overall, the Pegasus attacks on El Faro employees extended for eighteen months. A list of the known attacks against individuals in El Salvador, including Plaintiffs and other El

Faro employees, can be found in the Citizen Lab report summarizing the attacks, incorporated herein and attached hereto as Exhibit A.

60. Because Defendants intentionally designed Pegasus to avoid detection, El Faro and its employees were unaware during most of the time they were under attack that their devices had been compromised. El Faro's leadership learned of the first confirmed Pegasus attacks in October 2021, after the Citizen Lab, with the assistance of Access Now, detected evidence of Pegasus on the personal device of Plaintiff Julia Gavarrete. Upon receiving confirmation that her device had been infected with Pegasus, Ms. Gavarrete informed El Faro's leadership of the attack.

61. El Faro's leadership devoted considerable time and resources to identifying the full extent of the attacks and remediating the harms caused by them. The team—including Carlos Dada, Julia Gavarrete, Daniel Reyes Martínez, and Óscar Martínez—initially submitted forensic data from eleven devices used by El Faro employees for further analysis by the Citizen Lab, with the assistance of Access Now. After the Citizen Lab confirmed that all eleven devices had been infected with Pegasus, the team reached out to additional employees at risk of infection and submitted forensic data from thirty devices for analysis by December 2021. During that time and the months that followed, El Faro employees devoted hundreds of hours to investigating the attacks, identifying other employees who had been targeted, working with security researchers to confirm the nature and duration of the attacks, developing and implementing new digital security policies, and upgrading El Faro's information technology systems. As a result of the attacks, El Faro incurred significant costs that far exceeded $5,000 within the year after El Faro's leadership learned of the attacks.

62. The Pegasus attacks undermined El Faro's ability to operate, to support its employees, and to serve its readers. The attacks have diverted El Faro leadership and employees from reporting, editing, and publishing. Despite El Faro's best efforts, the attacks have deterred some sources from continuing to communicate with El Faro reporters, deterred some writers from publishing their work with El Faro, and deterred some advertisers from doing business with El Faro.

The Pegasus Attacks on Plaintiffs

63. The Pegasus attacks on devices used by Plaintiffs were part of a coordinated and sustained effort to undermine independent journalism in El Salvador. The attacks all unfolded in a similar manner, beginning with the deployment by Defendants and their clients of zero-click exploits to each targeted device. And the attacks caused similar damage to each device, compromising data stored on and accessible through it. The attacks disabled certain Apple iOS features on the devices, infected the devices with Pegasus, enabled Defendants and their clients to issue commands to the devices without Plaintiffs' knowledge or consent, and undermined the value of the devices for private communication and computing. Although Defendants designed Pegasus to leave no evidence of attempts to exfiltrate data from targeted devices, the Citizen Lab's analyses confirmed exfiltration of data from at least twelve of the devices targeted in the attacks against El Faro, including those used by Plaintiffs Sergio Arauz, Julia Gavarrete, Roman Gressier, Gabriel Labrador, Efren Lemus, Daniel Lizárraga, Carlos López Salamanca, Óscar Martínez, María Luz Nóchez, Mauricio Sandoval Soriano, and José Luis Sanz. On information and belief, Defendants and their clients exfiltrated data from all of Plaintiffs' targeted devices, including data stored on Plaintiffs' cloud-based accounts.

64. **Carlos Dada:** Carlos Dada is the co-founder and director of El Faro. His reporting focuses on corruption and violence.

65. Defendants and their clients hacked Mr. Dada's device, an iPhone 11 owned by El Faro, at least twelve times between July 2020 and June 2021.

66. During the relevant time period, Mr. Dada used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Facebook, Instagram, Signal, Telegram, Twitter, and WhatsApp. He used the device for communicating with family, friends, sources, and colleagues; for conducting online banking, planning travel, arranging transportation through ride-sharing apps, and consulting maps; and for storing videos and photos. He also used his device to communicate with sources, to store confidential and leaked documents, and to edit work-related documents and drafts in Google Drive. His device was connected to an iCloud account.

67. The Pegasus attacks caused Mr. Dada substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Mr. Dada's device. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately one hundred hours helping to lead El Faro's initial investigation into the attacks.

68. **Sergio Arauz:** Sergio Arauz is the deputy editor-in-chief of El Faro and has worked at the organization for twenty-two years. His reporting focuses on politics and human rights.

69. Defendants and their clients hacked Mr. Arauz's device, an iPhone 11 owned by El Faro, at least fourteen times between August 2020 and October 2021. The Citizen Lab confirmed that data was exfiltrated from Mr. Arauz's device in the course of these attacks, but it could not identify which data was stolen.

70. During the relevant time period, Mr. Arauz used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Facebook, Gmail, Instagram, Signal, Telegram, Twitter, and WhatsApp. He used the device to communicate with family and friends; to store personal financial information; and to conduct his work as a journalist, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts in Google Drive.

71. The Pegasus attacks caused Mr. Arauz substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes greatly diminished the value of Mr. Arauz's device, which he later replaced. He has suffered, and continues to suffer, mental anguish as a result of the attacks and the loss of his privacy. Finally, he incurred significant costs in investigating and remediating the attacks. For example, as a leader of El Faro and a member of El Faro's Board of Directors, he spent approximately two hundred hours investigating and remediating the attacks against the organization, including by participating in discussions about the impact of the attacks on El Faro and the safety of its employees. He also spent more than two

dozen hours investigating the scope of the attacks against his own device, including by reviewing his notes, project timelines, and reporting topics over the course of the attacks, by attending meetings regarding the forensic analysis of El Faro employees' devices, and by preparing a back-up of his own device for forensic analysis.

72. **Gabriela Cáceres Gutiérrez:** Gabriela Cáceres Gutiérrez is a reporter for El Faro. In 2021, she, along with Plaintiffs Carlos Martínez and Óscar Martínez, published one of El Faro's most significant investigations, revealing secret negotiations held in maximum security prisons between the Bukele Administration and incarcerated members of El Salvador's three main gangs: MS-13, Barrio 18 Revolucionarios, and Barrio 18 Sureños.

73. Defendants and their clients hacked Ms. Cáceres Gutiérrez's device, an iPhone 11 owned by El Faro, at least thirteen times between April and September 2021. These dates coincided with her investigation into the Bukele Administration's negotiations with Salvadoran gangs.

74. During the relevant time period, Ms. Cáceres Gutiérrez used her device, which was password-protected, extensively for both personal and professional purposes. Her device contained social media and messaging applications, including Instagram, Signal, Twitter, and WhatsApp. She used the device to communicate with family and friends; to store personal financial information; and to conduct her work as a journalist, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts in Google Drive. Her device was connected to an iCloud account.

75. The Pegasus attacks caused Ms. Cáceres Gutiérrez substantial harms. She has had to significantly alter how she uses her device, diminishing its value to her. She has suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, she incurred significant costs in investigating and remediating the attacks. For example, she spent approximately three weeks investigating the attacks and informing family, friends, and sources that their information had been exposed to Defendants and their clients. She also purchased a new iPhone to protect her sources following the attacks.

76. **Julia Gavarrete:** Julia Gavarrete joined El Faro's newsroom in 2021. Her reporting focuses on vulnerable communities in Central America, on women's rights, and on environmental issues.

77. Defendants and their clients hacked Ms. Gavarrete's personal device, an iPhone 11, as well as an El Faro–owned iPhone that she used for work, at least eighteen times between February and September 2021. At one point in 2021, after Ms. Gavarrete scheduled a meeting with a source using her device, military officers arrived at the meeting location at the scheduled time and prevented Ms. Gavarrete and her source from entering a building. The Citizen Lab confirmed that data was exfiltrated from Ms. Gavarrete's personal device in the course of these attacks, but it could not identify which data was stolen.

78. During the relevant time period, Ms. Gavarrete used her devices, both of which were password-protected, extensively. Her personal device contained social media and messaging applications, including Facebook, Instagram, Signal, Telegram, Twitter, and WhatsApp. She also used her personal device for emailing, conducting personal banking, storing photos of family and friends, sharing sensitive information about her father's failing health with family members and doctors, and monitoring footage from her home security camera. Her work device contained her work email, draft articles that were stored in Google Drive, photos of leaked documents that were stored on Google Photos, and work-related communications. She also used her work device to draft interview notes from anonymous sources. Both of her devices were connected to iCloud accounts.

79. The Pegasus attacks caused Ms. Gavarrete substantial harms. She has had to significantly alter how she uses both her personal and work devices, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Ms. Gavarrete's devices. She has also suffered, and continues to suffer, mental anguish and physical symptoms as a result of the attacks, including back pain and eye strain. Finally, she incurred significant costs in investigating and remediating the attacks. For example, she spent a month assisting in El Faro's investigation into the attacks, including by working with the Citizen Lab and Access Now, by meeting with El Faro's leaders and other

journalists to ascertain whether their devices had been attacked, and by informing her sources that their information had been exposed to Defendants and their clients. She also purchased an external hard drive so she could prepare back-ups of her devices for forensic analysis by the Citizen Lab, with the assistance of Access Now.

80. **Roman Gressier:** Roman Gressier is a reporter for El Faro. He writes El Faro's English-language newsletter and has reported extensively on Central American politics, human rights, and press freedom.

81. Defendants and their clients hacked Mr. Gressier's device, an iPhone 11 owned by El Faro, at least four times between May and June 2021. The Citizen Lab confirmed that data was exfiltrated from Mr. Gressier's device in the course of these attacks, but it could not identify which data was stolen.

82. During the relevant time period, Mr. Gressier used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Facebook, Facebook Messenger, Gmail, Instagram, ProtonMail, Signal, and WhatsApp. He used the device to communicate with family and friends; to store personal financial information and passwords; and to conduct his work as a journalist, including by communicating with anonymous sources and editing work-related documents and drafts in Google Drive. His device was connected to an iCloud account.

83. The Pegasus attacks caused Mr. Gressier substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Mr. Gressier's device. He has suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately sixty to seventy hours investigating the attacks, notifying contacts that their information had been exposed to Defendants and their clients, and attempting to remediate the attacks by improving his digital security.

84. **Gabriel Labrador:** Gabriel Labrador is a reporter for El Faro. He has reported extensively on criminal justice and public corruption, including on a Salvadoran Supreme Court

magistrate's ties to the MS-13 gang, on the political and policymaking roles of President Bukele's brothers, and on detentions during El Salvador's recent state of exception.

85. Defendants and their clients hacked Mr. Labrador's device, an iPhone 11 owned by El Faro, at least twenty times between August 2020 and November 2021. The Citizen Lab confirmed that data was exfiltrated from Mr. Labrador's device in the course of these attacks, but it could not identify which data was stolen.

86. During the relevant time period, Mr. Labrador used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Facebook, Facebook Messenger, Gmail, Google Hangouts, Google Meet, Instagram, Jitsi Meet, Snapchat, Skype, Telegram, Twitter, WhatsApp, and Zoom. He used the device to communicate with family and friends; to store personal financial information; and to conduct his work as a journalist, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts in Google Drive. His device was connected to iCloud and Dropbox accounts.

87. The Pegasus attacks caused Mr. Labrador substantial harms. He has had to significantly alter how he uses his device, including by minimizing communications with his sources. These necessary changes have greatly diminished the value of Mr. Labrador's device. He has suffered, and continues to suffer, mental anguish as a result of the attacks, and he has seen a therapist to help him manage this stress. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately twenty-four hours describing what he was working on when his device was infected with Pegasus. He spent approximately four hours attending meetings at El Faro about digital security in the wake of the attacks. He also purchased additional security software for his devices.

88. **Ana Beatriz Lazo Escobar:** Ana Beatriz Lazo Escobar is a marketing manager for El Faro, where she has worked for seven years.

89. Defendants and their clients hacked Ms. Lazo Escobar's device, an iPhone 11 owned by El Faro, at least once, in April 2021.

90. During the relevant time period, Ms. Lazo Escobar used her device, which was password-protected, extensively for both personal and professional purposes. Her device contained social media and messaging applications, including Gmail, Instagram, Signal, Telegram, Twitter, and WhatsApp. She also stored personal financial information on the device. Her device was connected to an iCloud account.

91. The Pegasus attack caused Ms. Lazo Escobar substantial harms. She has suffered, and continues to suffer, mental anguish as a result of the attacks, and she has seen a therapist to help her manage this stress. Finally, she incurred significant costs in investigating and remediating the attacks. For example, she spent approximately eight hours addressing the attacks, including by preparing a back-up of her device for forensic analysis.

92. **Efren Lemus:** Efren Lemus is a reporter for El Faro. His reporting focuses on gang violence and El Salvador's attempts to curtail it, as well as wrongdoing and corruption within the governing Nuevas Ideas party.

93. Defendants and their clients hacked Mr. Lemus's device, an iPhone 11 owned by El Faro, at least ten times between April and September 2021. The device was first infected with Pegasus on April 23, 2021, the day Mr. Lemus first received it from El Faro. Defendants and their clients hacked his device at least nine more times over the following five months. The Citizen Lab confirmed that data was exfiltrated from Mr. Lemus's device in the course of these attacks, but it could not identify which data was stolen.

94. During the relevant time period, Mr. Lemus used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Facebook, Google Meet, Signal, Telegram, Twitter, WhatsApp, and Zoom. He used the device to communicate with family and friends; to store personal financial information; and to conduct his work as a journalist, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts in Google Drive. His device was connected to an iCloud account.

95. The Pegasus attacks caused Mr. Lemus substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Mr. Lemus's device. He has suffered, and continues to suffer, great stress and uncertainty as a result of the attacks, leading him to avoid public places and to alter the route he takes when walking his daughters to school. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately one hundred hours addressing the attacks, including by assisting with El Faro's investigation into the attacks, suspending interviews on reporting projects out of fear of continued surveillance, and notifying sources and contacts that their information had been exposed to Defendants and their clients. He also purchased an external hard drive to prepare a back-up of his device for forensic analysis.

96. **Daniel Lizárraga:** Daniel Lizárraga worked as the investigations editor for El Faro from January to August 2021. His reporting focuses on corruption.

97. Defendants and their clients hacked Mr. Lizárraga's device, an iPhone 11 owned by El Faro, at least eight times between April and July 2021. The Citizen Lab confirmed that data was exfiltrated from Mr. Lizárraga's device in the course of these attacks, but it could not identify which data was stolen.

98. During the relevant time period, Mr. Lizárraga used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Signal, Telegram, Twitter, WhatsApp, and Zoom. He used the device to communicate with family and friends and to conduct his work with El Faro, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts in Google Drive. His device was connected to an iCloud account.

99. The Pegasus attacks caused Mr. Lizárraga substantial harms. He had to significantly alter how he uses his device, including by no longer using it for personal conversations and by minimizing work-related communications. He has suffered, and continues to suffer, mental anguish as a result of the attacks and the loss of his privacy, and he has seen a therapist to help him

manage this stress. He has also incurred significant costs in investigating and remediating the attacks. For example, he spent several hours addressing the attacks, including by preparing a back-up of his device for forensic analysis and by notifying contacts and sources that their information had been exposed to Defendants and their clients.

100. **Carlos López Salamanca:** Carlos López Salamanca is the general manager of El Faro.

101. Defendants and their clients hacked Mr. López Salamanca's device, an iPhone 11 owned by El Faro, at least three times between September 2020 and May 2021. The Citizen Lab confirmed that data was exfiltrated from Mr. López Salamanca's device in the course of these attacks, but it could not identify which data was stolen.

102. During the relevant time period, Mr. López Salamanca used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including FaceTime, Facebook, Gmail, Instagram, Signal, Telegram, Twitter, and WhatsApp. He used the device to communicate with family and friends; to store personal financial information and photographs; to order food using meal delivery applications; to read the news and watch videos; and to conduct his work with El Faro, including by storing confidential work-related documents in Google Drive. His device was connected to an iCloud account.

103. The Pegasus attacks caused Mr. López Salamanca substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and removing his work-related email account from his device altogether. These necessary changes greatly diminished the value of Mr. López Salamanca's device. He has suffered, and continues to suffer, mental anguish as a result of the attacks and the loss of his privacy. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately forty hours addressing the attacks, including by preparing a back-up of his device for forensic analysis. He spent approximately five additional hours notifying contacts that their information had been exposed to Defendants and their clients.

104. **Carlos Martínez:** Carlos Martínez is a reporter for El Faro. He is a founding member of El Faro's investigative journalism team, and his reporting focuses on gang violence and official misconduct.

105. Defendants and their clients hacked Mr. Martínez's device, an iPhone 11 owned by El Faro, at least twenty-eight times between June 2020 and October 2021. During many of these months, Mr. Martínez was in regular contact with U.S. Embassy officials as he investigated the Bukele Administration's negotiations with Salvadoran gangs. Although the Citizen Lab could not confirm whether data was exfiltrated from Mr. Martínez's device, one of El Faro's sources played Mr. Martínez's colleague an audio recording of a private conversation Mr. Martínez had with Óscar Martínez during this time.

106. During the relevant time period, Mr. Martínez used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Facebook, Facebook Messenger, Gmail, Instagram, Signal, Telegram, Twitter, and WhatsApp. He used the device to communicate with family and friends; to store personal financial information; and to conduct his work as a journalist, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts in Google Drive. His device was connected to an iCloud account.

107. The Pegasus attacks caused Mr. Martínez substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of his device. He has suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately five days informing family, friends, and sources that their information had been exposed to Defendants and their clients. He also purchased a new iPhone following the attacks.

108. **Óscar Martínez:** Óscar Martínez is the editor-in-chief of El Faro. A founding member El Faro's investigative journalism team, he reports on issues of gang violence, migration, and official misconduct.

109. Defendants and their clients hacked Mr. Martínez's device, an iPhone 8 owned by El Faro, at least forty-two times between July 2020 and October 2021. The Citizen Lab confirmed that data was exfiltrated from Mr. Martínez's device in the course of these attacks. Although the Citizen Lab could not identify which data was stolen from Mr. Martínez's device, one of El Faro's sources played Mr. Martínez's colleague an audio recording of a private conversation Mr. Martínez had with Carlos Martínez during this time.

110. During the relevant time period, Mr. Martínez used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Gmail, Signal, Telegram, Twitter, and WhatsApp. He used the device to communicate with family and friends; to store personal financial information; and to conduct his work as a journalist, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts.

111. The Pegasus attacks caused Mr. Martínez substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Mr. Martínez's device. He has suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent hundreds of hours investigating the attacks, developing El Faro's strategic response to the attacks, establishing new security protocols for El Faro, notifying contacts and sources that their information had been exposed to Defendants and their clients, and improving his own digital security. After the attacks, he started meeting with sources in person more frequently, increasing travel and booking costs. He also purchased at least ten different devices that he used in the months after the attacks were confirmed.

112. **María Luz Nóchez:** María Luz Nóchez is a reporter and the Opinion editor for El Faro. She reports on arts and culture, violence against women and the LGBTQ community, and the rights of Indigenous people.

113. Defendants and their clients hacked Ms. Nóchez's device, an iPhone 11 owned by El Faro, at least three times between February and June 2021. The Citizen Lab confirmed that data was exfiltrated from Ms. Nóchez's device in the course of these attacks, but it could not identify which data was stolen.

114. During the relevant time period, Ms. Nóchez used her device, which was password-protected, extensively for both personal and professional purposes. Her device contained social media and messaging applications, including FaceTime, Facebook Messenger, Gmail, Signal, Telegram, WhatsApp, and Zoom. She used the device to communicate with family and friends; to store personal financial information; and to conduct her work as a journalist, including by editing work-related documents and drafts in Google Drive. Her device was connected to an iCloud account.

115. The Pegasus attacks caused Ms. Nóchez substantial harms. She has had to significantly alter how she uses her device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of her device. She has also suffered, and continues to suffer, mental anguish and physical symptoms as a result of the attacks, including intense abdominal pain. She has seen a therapist to help her manage the stress resulting from the attacks. Finally, she incurred significant costs in investigating and remediating the attacks. For example, she spent several hours addressing the attacks, including by attending meetings at El Faro regarding the investigation into the attacks, preparing a back-up of her device for forensic analysis, and attending additional meetings about digital security following the attacks.

116. **Víctor Peña:** Víctor Peña is a photojournalist for El Faro. He contributes photography and audiovisual and graphic material to El Faro, focusing on issues relating to women's rights, inequality, pollution, and migration.

117. Defendants and their clients hacked Mr. Peña's device, an iPhone 11 owned by El Faro, at least once, on November 22, 2021. The attack on Mr. Peña's device was the last known Pegasus attack on El Faro.

118. During the relevant time period, Mr. Peña used his device, which was password-protected, extensively for personal and professional purposes. His device contained social media and messaging applications, including Facebook, Gmail, Instagram, Signal, Telegram, Twitter, and WhatsApp. He used the device to communicate with family and friends; to store personal financial information; and to conduct his work as a journalist, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts in Google Drive. His device was connected to an iCloud account.

119. The Pegasus attack caused Mr. Peña substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Mr. Peña's device. He has also suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately one month addressing the attacks, including by assisting with El Faro's investigation into the attacks and by notifying sources and contacts that their information had been exposed to Defendants and their clients.

120. **Nelson Rauda Zablah:** Nelson Rauda Zablah worked as a reporter and hosted a twice-weekly radio show for El Faro from 2015 to August 2022. He has a decade of experience covering corruption, crime, the justice system, politics, migration, and human rights.

121. Defendants and their clients hacked Mr. Rauda Zablah's device, an iPhone 11 owned by El Faro, at least six times between April and September 2021. The attacks against Mr. Rauda Zablah's device coincided with three dates on which he visited the U.S. Embassy in San Salvador.

122. During the relevant time period, Mr. Rauda Zablah used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Facebook, Gmail, Google Meet, Instagram,

Microsoft Teams, Skype, Telegram, TikTok, Twitter, WhatsApp, and Zoom. He used the device to communicate with family and friends, including receiving photos of his nieces and nephews; to store personal financial information; and to conduct his work as a journalist, including by communicating with anonymous sources, storing confidential and leaked documents, and editing work-related documents and drafts in Google Drive. His device was also connected to an iCloud account.

123. The Pegasus attacks caused Mr. Rauda Zablah substantial harms. He has had to significantly alter how he uses his device, including by no longer using it for personal communication or banking. Similarly, he began minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Mr. Rauda Zablah's device. He has suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately seventy hours assisting El Faro's investigation into the attacks, notifying contacts that their information had been exposed to Defendants and their clients, and taking remedial digital security measures. He spent approximately ten additional hours preparing a back-up of his device for forensic analysis, consulting with information technology experts, deleting and re-downloading the applications he had previously used, and conducting additional security analyses to check for any subsequent reinfection. After moving to the United States, he purchased a new, more secure device with a new number and cellular plan as a result of the attacks. Fearing that the new device may also be targeted, however, he does not use it for tasks that he routinely carried out on his previous device before the attacks.

124. **Daniel Reyes Martínez:** Daniel Reyes Martínez is the chief technology officer of El Faro.

125. Defendants and their clients hacked Mr. Reyes Martínez's device, an iPhone 11 owned by El Faro, at least twice between October 2020 and November 2021.

126. During the relevant time period, Mr. Reyes Martínez used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Telegram and WhatsApp. He used the device

to communicate with family and friends; to store personal financial information; and to conduct his work with El Faro, including by storing work-related documents and drafts in Google Drive. His device was connected to an iCloud account.

127. The Pegasus attacks caused Mr. Reyes Martínez substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and avoiding phone calls. These necessary changes greatly diminished the value of Mr. Reyes Martínez's device. He has suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, he incurred significant costs in investigating and remediating the attacks. For example, as chief technology officer of El Faro, he spent several months working full time to investigate and assess the extent of the Pegasus attacks. He also spent several hours investigating the scope of the attacks against his own device, including by purchasing a hard drive to prepare a back-up of his device for forensic analysis and by analyzing his device himself using a mobile verification toolkit created by Amnesty International. He also purchased a new device following the attacks in an attempt to ensure better digital security. Experiencing significant stress and uncertainty about the surveillance of his family as a result of the attacks, he also purchased security cameras and a smart doorbell for his home.

128. **Mauricio Ernesto Sandoval Soriano:** Mauricio Ernesto Sandoval Soriano is the general administrator of El Faro.

129. Defendants and their clients hacked Mr. Sandoval Soriano's device, an iPhone 11 owned by El Faro, at least four times between August 2020 and October 2021. The Citizen Lab confirmed that data was exfiltrated from Mr. Sandoval Soriano's device in the course of these attacks, but it could not identify which data was stolen.

130. During the relevant time period, Mr. Sandoval Soriano used his device, which was password-protected, extensively for work and occasionally for personal purposes. His device contained social media and messaging applications, including Gmail, Signal, Telegram, Twitter, and WhatsApp. He used his device to conduct his work, including by editing and signing documents in DocuSign and Google Drive and storing documents relating to El Faro's

administrative, financial, and strategic decisions; he also occasionally used his device for personal purposes, including to communicate with his wife and to share photographs.

131. The Pegasus attacks caused Mr. Sandoval Soriano substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Mr. Sandoval Soriano's device. He has also suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately fifty hours addressing the attacks, including by assisting with El Faro's investigation into the attacks. Experiencing significant stress and uncertainty about the surveillance of his family as a result of the attacks, he also purchased security cameras for his home.

132. **José Luis Sanz:** José Luis Sanz is the Washington correspondent for El Faro. Mr. Sanz reports on human rights, migration, and corruption. A founding member of El Faro's investigative journalism team, he previously reported on issues of violence, gangs, and organized crime in Central America.

133. Defendants and their clients hacked Mr. Sanz's device, an iPhone 8, at least thirteen times between July and December 2020. During these months, Mr. Sanz communicated and attended meetings with U.S. Embassy officials, as well as diplomatic representatives from the European Union, France, Spain, and the United Kingdom. The Citizen Lab confirmed that data was exfiltrated from Mr. Sanz's device in the course of these attacks, but it could not identify which data was stolen.

134. During the relevant time period, Mr. Sanz used his device, which was password-protected, extensively for both personal and professional purposes. His device contained social media and messaging applications, including Facebook, Gmail, Instagram, Signal, Skype, Telegram, Twitter, and WhatsApp. He used the device to communicate with family and friends; to store photographs; to store personal financial information; and to conduct his work as a journalist, including by maintaining the contact information of anonymous sources and editing

work-related documents and drafts in Google Drive. His device was also connected to an iCloud account.

135. The Pegasus attacks caused Mr. Sanz substantial harms. He has had to significantly alter how he uses his device, including by minimizing work-related communications and prioritizing in-person meetings. These necessary changes have greatly diminished the value of Mr. Sanz's device. He has also suffered, and continues to suffer, mental anguish as a result of the attacks. Finally, he incurred significant costs in investigating and remediating the attacks. For example, he spent approximately eighty hours assisting El Faro's investigation into the attacks and taking remedial digital security measures. He spent approximately four to five additional hours notifying contacts and sources that their information had been exposed to Defendants and their clients.

136. Overall, the Pegasus attacks caused Plaintiffs serious economic, reputational, professional, psychological, and personal harms, and caused Plaintiffs and El Faro significant losses aggregating over $5,000 within the year after they learned of the attacks. The attacks have also undermined Plaintiffs' ability to serve as sources of independent journalism in El Salvador and Central America.

CAUSES OF ACTION

Count I
Violations of the Computer Fraud and Abuse Act
18 U.S.C. § 1030

137. As explained above, between June 2020 and November 2021, Defendants repeatedly accessed Plaintiffs' devices, including their cloud-based accounts, without authorization. Each Plaintiff either owned a device targeted in the Pegasus attacks or had a possessory interest in and exclusive right to use a targeted device in connection with their employment with El Faro. These devices also contained Plaintiffs' private information, including private communications, photographs, and writings. The devices are "protected computers" within the meaning of 18 U.S.C. § 1030(e)(2)(B) because they are "used in or affecting interstate or foreign commerce or communication."

138. Plaintiffs suffered both damage and loss as a result of the Pegasus attacks on their devices.

139. The total losses stemming from the Pegasus attacks—including costs incurred by Plaintiffs as well as those incurred by El Faro—exceeded $5,000 in aggregate during a one-year period.

140. The Pegasus attacks damaged the devices used and/or owned by Plaintiffs. For example, the attacks disabled certain Apple iOS features on the devices, infected the devices with spyware, and enabled Defendants and their clients to issue commands to the devices without Plaintiffs' knowledge or consent—all of which also made the devices less valuable to Plaintiffs as tools for private communication and computing.

18 U.S.C. § 1030(a)(2)(C)

141. Defendants violated 18 U.S.C. § 1030(a)(2)(C) because they intentionally accessed and/or caused to be accessed Plaintiffs' devices without authorization and obtained information from those devices.

142. Defendants accessed and/or caused to be accessed Plaintiffs' devices without authorization through attacks that enabled the surreptitious installation of Pegasus on Plaintiffs' devices.

143. Defendants infected Plaintiffs' devices with Pegasus to enable real-time surveillance of those devices and to exfiltrate data from those devices to Defendants and their clients. Once installed, Pegasus provided Defendants and their clients with essentially unlimited access to Plaintiffs' devices, allowing them to remotely surveil and exfiltrate data stored on those devices and on the cloud-based accounts connected to those devices.

144. Although Pegasus attacks are designed to leave no trace, analysis by the Citizen Lab confirmed that data was obtained from at least eleven devices used and/or owned by Plaintiffs. On information and belief, Defendants and their clients obtained data from all of Plaintiffs' targeted devices, including by accessing data stored on Plaintiffs' cloud-based accounts.

18 U.S.C. § 1030(a)(5)

145. Defendants violated 18 U.S.C. § 1030(a)(5)(A) because they knowingly caused the transmission of a program, information, code, or command to Plaintiffs' devices and, as a result, intentionally damaged those devices without authorization.

146. Defendants violated 18 U.S.C. § 1030(a)(5)(B) because they intentionally accessed Plaintiffs' devices without authorization and, as a result, recklessly caused damage.

147. Defendants violated 18 U.S.C. § 1030(a)(5)(C) because they intentionally accessed Plaintiffs' devices without authorization and, as a result, caused damage and loss.

18 U.S.C. § 1030(b)

148. Defendants violated 18 U.S.C. § 1030(b) by conspiring and attempting to commit the violations alleged in the preceding paragraphs.

149. In the alternative, Defendants knowingly and intentionally aided and abetted their clients in the violations of 18 U.S.C. § 1030 alleged in the preceding paragraphs.

Count II
Violations of the California Comprehensive Computer Data Access and Fraud Act
California Penal Code § 502

150. Each Plaintiff either owned a device targeted in the Pegasus attacks or had a possessory interest in and exclusive right to use a targeted device in connection with their employment with El Faro. These devices also contained Plaintiffs' private information, including private communications, photographs, and writings.

151. Defendants violated California Penal Code § 502(c)(1) by knowingly and without permission accessing Plaintiffs' devices and altering, damaging, or using those devices in order to wrongfully control the devices and obtain data from them. Analysis by the Citizen Lab confirmed that data was obtained from at least eleven of Plaintiffs' devices. On information and belief, Defendants and their clients obtained data from all of Plaintiffs' targeted devices, including by accessing information stored on Plaintiffs' cloud-based accounts.

152. Defendants violated California Penal Code § 502(c)(2) by knowingly accessing and without permission taking, copying, and making use of data from Plaintiffs' devices, including data stored on their cloud-based accounts.

153. Defendants violated California Penal Code § 502(c)(3) by knowingly accessing and without permission using, or causing to be used, Plaintiffs' computer services. The installation of Pegasus on Plaintiffs' devices required computing and data processing by the targeted devices without Plaintiffs' knowledge or consent. The installation and maintenance of Pegasus on Plaintiffs' devices relied on and exploited the devices' storage functions without Plaintiffs' knowledge or consent. The exfiltration of data from Plaintiffs' devices resulted from Pegasus issuing commands to the devices and controlling their computing functions without Plaintiffs' knowledge or consent.

154. Defendants violated California Penal Code § 502(c)(4) by knowingly accessing and without permission adding and altering data, software, and computer programs on Plaintiffs' devices. Defendants altered the functioning of Plaintiffs' devices by infecting them with malicious data, software, and computer programs without Plaintiffs' permission.

155. Defendants violated California Penal Code § 502(c)(6) by knowingly providing a means of accessing Plaintiffs' devices and cloud-based accounts in violation of the California Computer Data Access and Fraud Act.

156. Defendants violated California Penal Code § 502(c)(7) by knowingly and without permission accessing and causing to be accessed Plaintiffs' devices and cloud-based accounts.

157. Defendants violated California Penal Code § 502(c)(8) by knowingly introducing a computer contaminant onto Plaintiffs' devices.

158. In carrying out the attacks on Plaintiffs' devices, Defendants acted oppressively, fraudulently, and maliciously.

Count III
Trespass to Chattels

159. Each Plaintiff either owned a device targeted in the Pegasus attacks or had a possessory interest in and exclusive right to use a targeted device in connection with their employment with El Faro. These devices also contained Plaintiffs' private information, including private communications, photographs, and writings.

160. Through the Pegasus attacks, Defendants intentionally and without authorization interfered with Plaintiffs' possessory interest in the targeted devices and in the information stored on and accessible through those devices.

161. Through the Pegasus attacks, Defendants intentionally and without authorization damaged the devices used and/or owned by Plaintiffs. For example, the attacks disabled certain Apple iOS features on the devices, infected the devices with spyware, and enabled Defendants and their clients to issue commands to the devices without Plaintiffs' consent—all of which also made the devices less valuable to Plaintiffs as tools for private communication and computing.

162. Defendants caused Plaintiffs to suffer substantial harms, including the degradation in value of the devices themselves, costs incurred in investigating and remediating the attacks, loss of professional goodwill, medical expenses, and emotional distress.

Count IV
Intrusion upon Seclusion

163. Each Plaintiff either owned a device targeted in the Pegasus attacks or had a possessory interest in and exclusive right to use a targeted device in connection with their employment with El Faro. Plaintiffs had a reasonable expectation of privacy in these devices. Each device was password-protected and contained private information, including communications, photographs, and writings.

164. Defendants intentionally intruded into Plaintiffs' private affairs by installing or causing to be installed malicious code on their devices. The installation of Pegasus on Plaintiffs' devices gave Defendants and their clients essentially full control of the devices, including the ability to covertly surveil and extract contact details, text messages, instant messages, notes, emails, web-browsing activity, files, and passwords; to monitor phone calls and VoIP calls, as well as user activity on different applications, including WhatsApp, Facebook, and Skype; to track and log the device's GPS location; to activate the device's microphone to record surrounding sounds; and to activate the device's camera to take photographs. Although Pegasus attacks are designed to leave no trace, the Citizen Lab's analyses confirmed that data was exfiltrated from at least eleven devices used and/or owned by Plaintiffs. On information and belief, Defendants and their clients

exfiltrated data from all of Plaintiffs' targeted devices, including by accessing data stored on their cloud-based accounts.

165. Defendants' actions would be highly offensive to the reasonable person.

166. The Pegasus attacks executed by Defendants and their clients caused Plaintiffs to suffer substantial harms, including the degradation in value of the devices themselves, costs incurred in investigating and remediating the attacks, medical expenses, and emotional distress.

REQUEST FOR RELIEF

Plaintiffs respectfully request that this Court:

A. Declare that Defendants have:

i. Violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

ii. Violated the California Comprehensive Computer Data Access and Fraud Act, Cal. Penal Code § 502;

iii. Trespassed onto Plaintiffs' property in violation of California law; and

iv. Intruded upon Plaintiffs' seclusion in violation of California law.

B. Enter a permanent injunction restraining Defendants from accessing, attempting to access, or assisting others in accessing or attempting to access, Plaintiffs' devices.

C. Enter a permanent injunction requiring Defendants to catalogue all information obtained as a result of the Pegasus attacks on Plaintiffs' devices; to return and then delete all such information in Defendants' possession; to disclose the identities of all persons and/or entities with whom Defendants shared such information, when that information was shared, and under what conditions; and to disclose the identities of all of Defendants' clients who were involved in the attacks on Plaintiffs' devices, including the specific individuals with whom Defendants contracted or coordinated and the specific nature of each individual's involvement.

D. Award Plaintiffs compensatory damages, as permitted by law and in such amounts to be proven at trial.

E. Award Plaintiffs punitive damages, as permitted by law and in such amounts to be proven at trial.

F. Award Plaintiffs their reasonable costs and attorneys' fees incurred in this action.

G. Grant such other and further relief as the Court may deem just and proper.

DATED: December 16, 2022

Respectfully submitted,

/s/ Paul Hoffman

Paul Hoffman #71244
John Washington #315991
Schonbrun, Seplow, Harris,
Hoffman & Zeldes LLP
200 Pier Avenue, Suite 226
Hermosa Beach, CA 90254
T: (424) 297-0114
F: (310) 399-7040
hoffpaul@aol.com

/s/ Carrie DeCell

Carrie DeCell, *Pro Hac Vice*
Jameel Jaffer, *Pro Hac Vice*
Alex Abdo, *Pro Hac Vice*
Stephanie Krent, *Pro Hac Vice*
Evan Welber Falcón, *Pro Hac Vice*
Knight First Amendment Institute
at Columbia University
475 Riverside Drive, Suite 302
New York, NY 10115
T: (646) 745-8500
F: (646) 661-3361
carrie.decell@knightcolumbia.org

Counsel for Carlos Dada, Sergio Arauz, Gabriela Cáceres Gutiérrez, Julia Gavarrete, Roman Gressier, Gabriel Labrador, Ana Beatriz Lazo Escobar, Efren Lemus, Daniel Lizárraga, Carlos López Salamanca, Carlos Martínez, Óscar Martínez, María Luz Nóchez, Víctor Peña, Nelson Rauda Zablah, Daniel Reyes Martínez, Mauricio Sandoval Soriano, and José Luis Sanz

EXHIBIT A

Project Torogoz

Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware

By John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ron Deibert

JANUARY 12, 2022
RESEARCH REPORT #148

munk school OF GLOBAL AFFAIRS & PUBLIC POLICY
UNIVERSITY OF TORONTO
THECITIZENLAB

Copyright

© Citizen Lab



Licensed under the Creative Commons BY-SA 4.0 (Attribution-ShareAlike licence). Electronic version first published in 2022 by the Citizen Lab. This work can be accessed through https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/.

Document Version: 1.0

The Creative Commons Attribution-ShareAlike 4.0 license under which this report is licensed lets you freely copy, distribute, remix, transform, and build on it, as long as you:

- give appropriate credit;
- indicate whether you made changes; and
- use and link to the same CC BY-SA 4.0 licence.

However, any rights in excerpts reproduced in this report remain with their respective authors; and any rights in brand and product names and associated logos remain with their respective owners. Uses of these that are protected by copyright or trademark rights require the rightsholder's prior written agreement.

Suggested Citation

John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Al-Jizawi, Salvatore Solimano, and Ron Deibert. "Project Torogoz: Extensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware," Citizen Lab Research Report No. 148, University of Toronto, January 2022.

Acknowledgements

We thank and acknowledge the many individuals that allowed us to analyze their devices as part of this investigation.

Special thanks to Mohammed Al-Maskati from Frontline Defenders for invaluable assistance.

Special thanks to the staff and incident handlers at the Access Now helpline for their invaluable support to this process and assistance to victims.

Special thanks to all of the organizations participating in this investigative collaboration including SocialTIC and Fundación Acceso.

Thanks to Siena Anstis, Celine Bauwens, Miles Kenyon, Adam Senft, and Mari Zhou for review, copy editing, and publication support.

Special thanks to TNG for invaluable assistance on this project.

About the Citizen Lab, Munk School of Global Affairs & Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

Key Findings 1

1. Introduction 1

Repression and Impunity in El Salvador 2
The Bukele Administration 2
The State of Police and Private Security Firms 3
Salvadoran Media under Threat 4
The TOROGOZ Pegasus Operator and El Salvador 4

2. Findings: Salvadoran Pegasus Targeting 5

Confirmed Targets 5
Zero-Click Exploits 7
One-Click Links 7

3. Attribution 8

4. Conclusion: Mercenary Spyware Continues to Harm Media, Civil Society 9

Pegasus and the Media 10

Appendix A: Hacking Timeline 10

Proyecto Torogoz: Hackeo extensivo de los medios de comunicación y la sociedad civil en El Salvador con el programa espía Pegasus

Key Findings

- **The Citizen Lab and Access Now have conducted a joint investigation into Pegasus hacking in El Salvador in collaboration with Frontline Defenders, SocialTIC, and Fundación Acceso.**
- **We confirmed 35 cases of journalists and members of civil society whose phones were successfully infected with NSO's Pegasus spyware between July 2020 and November 2021. We shared a sample of forensic data with Amnesty International's Security Lab which independently confirms the findings.**
- **Targets included journalists at *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, *Revista Digital Disruptiva*, *Diario El Mundo*, *El Diario de Hoy*, and two independent journalists. Civil society targets included *Fundación DTJ, Cristosal*, and another NGO.**
- **The hacking took place while the organizations were reporting on sensitive issues involving the administration of President Bukele, such as a scandal involving the government's negotiation of a "pact" with the MS-13 gang for a reduction in violence and electoral support.**
- **While evidence linking a particular infection to a particular Pegasus customer is often unavailable, in this case we identified a Pegasus customer operating almost exclusively in El Salvador since at least November 2019 that we call TOROGOZ, and have connected this operator to an infection attempt against *El Faro*.**

1. Introduction

This report describes the results of a collaborative investigation into the abuse of NSO Group's Pegasus spyware to target members of the press and civil society in El Salvador. The investigation led to the identification of 35 Pegasus-infected individuals (37 devices) among members of El Salvador's media and civil society.

Our investigation began in September 2021 when a group of independent journalists contacted Access Now's Digital Security Helpline after testing their devices using the Amnesty International Security Lab's Mobile Verification Toolkit (MVT) tool to detect Pegasus spyware.

The resulting investigation was a collaboration between the Citizen Lab and Access Now, with investigative assistance and case referrals from Frontline Defenders, SocialTIC, and Fundación Acceso. We asked Amnesty International's Security Lab to conduct an independent review of our analysis for a sample of cases, and they have confirmed our findings.

Repression and Impunity in El Salvador

Like most central American countries, El Salvador has had a troubled history marked by authoritarianism, endemic civil war and numerous coups, official and clandestine foreign intelligence and military assistance (particularly during the Cold War), organized crime, corruption, and drug trafficking.

Between 1970 and 1992, the country was ravaged by the Salvadoran Civil War, fought between a right-wing military junta and a coalition of left-wing guerilla groups under the umbrella of the Farabundo Martí National Liberation Front (FMLN). The era was characterized by frequent extra-judicial killings, mass disappearances and massacres of civilians, and numerous other human rights abuses, many of which were undertaken by “death squads” (some of whom were reportedly supported and trained by United States military advisors).

This period of violence and authoritarianism left a deep legacy of impunity and a tradition of corruption in El Salvador’s armed forces and political establishment. The period also created opportunities for organized crime and corruption, as well as the growth of poorly regulated and unaccountable private security firms.

The Bukele Administration

El Salvador's current president is the charismatic 40 year old Nayib Bukele, who has been in office since winning the general election in June 2019. Bukele was formerly mayor of Nuevo Cuscatlán (2012-15) and mayor of San Salvador (2015-18). In both cases he represented leftist parties. Although Bukele represents an aesthetic break with the typical Latin American autocrat, and despite his many public denouncements against strongmen, he has shown growing autocratic tendencies.

In February 2020, Bukele entered the legislative assembly accompanied by soldiers and armed guards in an attempt to intimidate lawmakers into approving his platform. In May 2021, Bukele and his supporters in the legislature fired the country’s attorney general and several judges, in a move that Bukele described as "cleaning our house." Bukele was elected on a platform that included a plan to reduce the extraordinary violence in the country by encouraging cooperation between the country’s armed forces and organized criminal gangs.

Although official murder counts have declined in recent years, a 2021 report by the Foundation of Studies for the Application of Law (Fundación de Estudios para la Aplicación del Derecho, or FESPAD) found that pacts between gangs and state officials, originally intended to lower homicide rates, have instead increased the recurrence of forced disappearances. FESPAD found several unidentified mass graves in areas with the highest gang presence. While forced disappearances allow gangs to execute with impunity, Bukele’s administration also undertakes brutal crackdowns against imprisoned gang members across the country.

Unlike many past authoritarians, Bukele blends a particular fluency in social media and dexterity in the use of memes, with the use of large popular public events to capitalize on popular disenchantment with traditional political parties. A recent analysis described Bukele as embodying a new type of "millennial authoritarianism," defined as "a distinctive political strategy that combines traditional populist appeals, classic authoritarian behavior, and a youthful and modern personal brand built primarily via social media."

The State of Police and Private Security Firms

The policing of gang violence within a context of generalized insecurity in El Salvador warrants special attention. In 2019, President Bukele authorized the intervention of armed forces in police duties, resulting in numerous human rights concerns, as highlighted in a 2020 State Dept. Human Rights report. At present, Salvadorans are concurrently subjected to both gang violence and aggressive, authoritarian policing. The threat of violence has led to unprecedented internal displacement. In 2017 alone, 296,000 Salvadorans were forced to move out of their homes due to the threat of violence.

Approximately 450 private security firms are operating illegally in El Salvador, often due to a failure to obtain or renew proper authorization and paperwork. Salvadoran police claim to be unable to hold these firms accountable. As of 2016, roughly 24,100 private security guards were active in El Salvador, an estimate that dwarfs the number of active police officers.

With private security firms and militia lacking proper oversight, El Salvador's Private Security Services Law does little to solve the problem, as noted by Freedom House. Article 47 of this law indicates that severe offenses attributed to private security services must be sanctioned with a financial penalty on salaries, but the exact nature of the fine is vague. This gap leaves police forces unable to hold private security firms accountable for their conduct. *La Prensa Gráfica* has found that not a single private security firm has been held accountable. Instances where police did come close to sanctioning a firm were later dropped in court.

This lack of accountability is troubling in light of accounts that Mara Salvatrucha (MS-13) gang members have infiltrated private security firms to extort Salvadoran citizens. Indeed, extortion has been on the rise since the Salvadoran government struck a deal with gang leaders. Salvadoran police have also had trouble keeping their own personnel in check. For example, a 2017 *Insight Crime* report shows that while some police officers have been jailed for illegal smuggling of items into jail cells, others, accused of extrajudicial killings, remain free.

Salvadoran Media under Threat

While there is a lively press in El Salvador, with outlets such as *El Faro* and *Revista Factum* providing regular critical coverage, journalists face numerous challenges in the country.

Reporters Without Borders ranks El Salvador 82nd in its 2021 World Press Freedom Index (an eight-place drop since 2020). Freedom House ranks El Salvador's freedom and independence of media as "partially free" and highlights rampant corruption, censorship, and interventions such as barring access to journalists at homicide scenes. Both *El Faro* and *Revista Factum* have also been frequently barred from accessing government conferences. The Freedom House report also notes verbal attacks directed at the press by Bukele himself. For example, in September 2020, Bukele used two hours of national airtime to denigrate and accuse the media of being his enemies.

Verbal attacks and threats against the press are not limited to Bukele. In September 2021, Javier Argueta, Nayib Bukele's legal counsel, threatened two journalists at *GatoEncerrado* for reporting on a meeting he held with four members of the Salvadoran Supreme Electoral Court. In a Twitter diatribe, Argueta threatened legal action if the journalists did not reveal their sources.

In 2021 alone, the Journalists Association of El Salvador (APES) recorded more than 200 cases of aggression against journalists, ranging from denial of access to harassment. Instances of animosity toward the press have involved state ministers and legislators, as well as executives of El Salvador's Autonomous Executive Port Commission (CEPA), all found to have verbally abused reporters. June and July 2021 press releases from APES denounced abuses by members of the Supreme Court of Justice, Bukele's Office and the Ministry of Security and Justice. In addition, a 165% increase in aggressions against female journalists, recorded last year, also characterizes El Salvador's endemic problem of media repression.

The TOROGOZ Pegasus Operator and El Salvador

Through our ongoing Internet scanning and DNS cache probing, we identified a Pegasus operator focusing almost exclusively within El Salvador that we named ***TOROGOZ***. We first observed this operator in early 2020, though the domain names associated with the operator appear to have been registered as early as November 2019.

In a 2020 report *Running in Circles*, we identified a Salvadoran client of Circles, an NSO Group-affiliated company. The Circles system, which is an entirely separate product and uses different technology than Pegasus, allows its operator to track locations of phones around the world, and to intercept unencrypted SMS messages and phone calls in some cases. Unlike Pegasus, use of the Circles system does not involve hacking target devices, and instead involves attacks against the mobile phone signaling system. The forensic artifacts analyzed in this report have no relationship to Circles technology.

While there is no conclusive technical evidence that ***TOROGOZ*** represents the Salvadoran government, the strong country-specific focus of the infections suggests that this is very

likely. Additionally, in the single case of hacking in this investigation in which we recovered the domain names of the Pegasus servers used, the ***TOROGOZ*** operator was implicated.

2. Findings: Salvadoran Pegasus Targeting

Following the Citizen Lab's research and technical protocols, the Citizen Lab and Access Now obtained forensic artifacts, including logs, from each target's device. With their consent, we analyzed the logs for forensic signatures associated with NSO Group's Pegasus spyware.

We conclude that at least 35 individuals from media organizations *El Faro*, *GatoEncerrado*, *La Prensa Gráfica*, *Revista Digital Disruptiva*, *Diario El Mundo*, *El Diario de Hoy,* and two independent journalists were hacked with Pegasus. We also identified hacking against civil society organizations in El Salvador, including Fundación DTJ, Cristosal, and another NGO.

The infections described in this report have been identified with high confidence and a sample of the cases have been peer reviewed by Amnesty's Security Lab. Their peer review supports our finding of Pegasus infections.

Confirmed Targets[1]

Our forensic analysis focuses on determining whether specific processes or binaries linked to NSO Group's Pegasus spyware were running on the phone in question during a specified time. The forensic analysis involves both searching records of execution maintained by the phone, as well as searching for other traces associated with the execution or installation of Pegasus. See **Appendix A** for a full list of dates that exploits were fired at the phones resulting in successful hacking.

Pegasus attempts to delete evidence of its successful exfiltration, so evidence establishing exfiltration may not be available in all cases. This should not be interpreted as suggesting that exfiltration did not take place.

Target	Affiliation	Forensic Finding
Noah Bullock	Cristosal	Pegasus infection
(Individual #1)	Diario El Mundo	Pegasus infection
Ricardo Avelar	El Diario de Hoy	Pegasus infection
Ana Beatriz Lazo	El Faro	Pegasus infection
Carlos Dada	El Faro	Pegasus infection
Carlos Ernesto Martínez D'aubuisson	El Faro	Pegasus infection
Daniel Lizárraga	El Faro	Pegasus exfiltration

1 Whereas a number of targets preferred to remain anonymous, the other targets consented to be identified.

Target	Affiliation	Forensic Finding
Daniel Reyes	El Faro	Pegasus infection
Efren Lemus	El Faro	Pegasus exfiltration
Gabriel Labrador	El Faro	Pegasus exfiltration
Gabriela Cáceres	El Faro	Pegasus infection
José Luis Sanz	El Faro	Pegasus exfiltration
Julia Gavarrete (Phone #1)	El Faro	Pegasus exfiltration
Julia Gavarrete (Phone #2)	El Faro	Pegasus infection
María Luz Nóchez	El Faro	Pegasus exfiltration
Mauricio Ernesto Sandoval Soriano	El Faro	Pegasus exfiltration
Nelson Rauda	El Faro	Pegasus infection
Óscar Martínez	El Faro	Pegasus exfiltration
Rebeca Monge	El Faro	Pegasus infection
Roman Gressier	El Faro	Pegasus exfiltration
Roxana Lazo	El Faro	Pegasus exfiltration
Sergio Arauz	El Faro	Pegasus exfiltration
Valeria Guzmán	El Faro	Pegasus infection
Víctor Peña	El Faro	Pegasus infection
(Individual #2)	El Faro	Pegasus infection
(Individual #3)	El Faro	Pegasus exfiltration
Jose Marinero	Fundación DTJ	Pegasus infection
Xenia Hernandez	Fundación DTJ	Pegasus infection
Beatriz Benitez	GatoEncerrado	Pegasus exfiltration
Ezequiel Barrera	GatoEncerrado	Pegasus exfiltration
Xenia Oliva (Phone #1)	GatoEncerrado	Pegasus exfiltration
Xenia Oliva (Phone #2)	GatoEncerrado	Pegasus exfiltration
(Individual #4)	La Prensa Gráfica	Pegasus infection
Oscar Luna	Revista Digital Disruptiva	Pegasus infection
(Individual #5)	(NGO #1)	Pegasus infection
Mariana Belloso	(Independent Journalist)	Pegasus infection
Carmen Tatiana Marroquín	(Economist and Columnist for Independent Media)	Pegasus infection

Table 1: Confirmed individuals hacked with Pegasus Spyware in El Salvador.

Each positive result in this case represents a phone we identified with *high confidence* as successfully hacked with Pegasus spyware (denoted as “Pegasus infection” in **Table 1**). In a subset of the cases, we are able to establish an additional result: successful exfiltration (denoted as “Pegasus exfiltration” in **Table 1**), indicating high confidence that the spyware successfully uploaded data from the phone to Pegasus infrastructure. In several

cases, Pegasus apparently exfiltrated multiple gigabytes of data successfully from target phones using their mobile data connections.

We observed extensive targeting using zero-click exploits, however we also identified specific instances in which targets were sent one-click infection links via SMS message.

Zero-Click Exploits

We assess that at least two zero-click exploits were deployed against the journalists in El Salvador: ***KISMET*** and ***FORCEDENTRY***. Thirteen of the phones contained the ***KISMET FACTOR***, which we believe is an artifact left behind by the execution of NSO Group's zero-click ***KISMET*** exploit. We saw this exploit deployed between July and December 2020, and the exploit appears to have been a zero-day against iOS 13.5.1 and 13.7. The ***KISMET*** exploit has not yet been publicly captured and analyzed, but appeared to involve the use of JPEG attachments, as well as iMessage's *IMTranscoderAgent* process invoking a WebKit instance.

Additionally, we recovered a copy of the ***FORCEDENTRY*** exploit from one of the phones. The exploit appears to have been fired at a phone with iOS 14.8.1, which is not vulnerable to ***FORCEDENTRY***. The exploit does not appear to have run on the phone. It is unclear why the exploit was fired at a non-vulnerable iOS version, though it is possible that NSO operators cannot always determine the precise iOS version used by the target before firing an exploit.

We have not identified a long-lived forensic artifact associated with ***FORCEDENTRY*** that can differentiate that exploit from other techniques used to install Pegasus on a phone, but we believe that NSO iPhone hacking between February and November 2021 was generally conducted with the ***FORCEDENTRY*** exploit. ***FORCEDENTRY*** appears to be the same exploit that Amnesty's Security Lab observed traces of in their Pegasus Project analysis, which they refer to as "Megalodon."

One-Click Links

We fingerprinted Pegasus URL shortener websites and identified 244 domain names registered from 2019 through 2021 that appear to have been used by various NSO Group customers to distribute the Pegasus spyware via links. In the case of a single target at El Faro, we saw one-click SMS messages sent to the target containing links matching our Pegasus fingerprint.

Date	Original SMS	English Translation
Jul 4, 2020	Fiscalia tras periodistas del faro. https://info-urbano[.]com/SxUqnKe1	District attorney's office against journalists from El Faro

Date	Original SMS	English Translation
Jul 4, 2020	Personal de salud denuncia mala administracion del Gobierno https://informados24h[.]com/wNjzhTb	Health staff denounces bad administration by the government
Jul 7, 2020	Presidente sale en defensa de su ahijado politico. https://informados24h[.]com/ZKtywtTbM	The President comes out in defense of his political protégé
Jul 8, 2020	Nuevas Ideas eclipsa a sus oponentes. https://informados24h[.]com/VNCeEmT	Nuevas Ideas [the political party of El Salvador's President] eclipses their opponents
Sep 7, 2020[2]	Noticia de El Salvador trasciende a nivel mundial https://informados24h[.]com/nRG9mDx	News from El Salvador goes worldwide

The messages sent to the target contained links to the following Pegasus domain names:

```
informados24h[.]cominfo-urbano[.]com
```

The following four domains that we detected in our Pegasus scanning had similar registration characteristics to the two domains above above and thus may have been used by the same Pegasus customer:

```
mobile-analytics[.]netweb-cloud-services[.]com
```

```
solo-hoy[.]com
```

```
deportes24-7[.]com
```

Apple Notifications to Confirmed Pegasus Victims

On November 23rd, 2021 Apple began sending notifications to some iPhone users who had been targeted with NSO Group's ***FORCEDENTRY*** exploit. Apple also filed a lawsuit against NSO Group on the same day.

Many of the Pegasus targets that we confirm in this investigation also reported receiving "state-sponsored spyware" notifications from Apple, including twelve journalists at *El Faro*, and two members of *Fundación DTJ*.

3. Attribution

At this time Citizen Lab is not conclusively attributing the attacks to a particular government customer of NSO Group, however there is a range of circumstantial evidence pointing to a strong El Salvador government nexus.

2 Note that the original SMS contains a double-space between the words "Salvador" and "trasciende"

First, the cases share a troubling nexus with the interests of the Bukele government:

- Targeting coincides with moments that the organizations were working on issues of great interest to the Bukele government
- Targets work focuses on domestic issues, and thus would be most relevant to a domestic audience

Secondly, Citizen Lab network scanning-based evidence has revealed TOROGOZ, an operator whose activities are strongly suggestive of a Pegasus customer in El Salvador. Notably, the operator had a near-total focus of infections within El Salvador, which is strongly suggestive of a domestic Pegasus operator.

Thirdly, one of the targets at *El Faro* (Carlos Martínez) was targeted by TOROGOZ in an unsuccessful attempt with the ***FORCEDENTRY*** exploit. The exploit was fired at a non-vulnerable version of iOS (14.8.1).

4. Conclusion: Mercenary Spyware Continues to Harm Media, Civil Society

For years, researchers and civil society have sounded the alarm that the poorly regulated mercenary surveillance market is leading to widespread human rights and other abuses. The El Salvador case presents a textbook example of those concerns.

If indeed Pegasus was sold to El Salvador, it was done despite a panoply of warning signs that abuse would take place:

- An autocratic leaning President with a fascination with digital technology
- A long history of harassment of independent media and journalists
- A climate of insecurity and human rights abuses
- Poorly regulated police, intelligence, and private security firms
- A lengthy history of corruption, organized crime, state violence, and authoritarianism

The hacking of Salvadoran civil society organizations with Pegasus mercenary spyware reflects a familiar pattern observed time and again in authoritarian societies: the use of advanced technology to frustrate and interfere with this essential component of a democratic society. In this case, the hacking also fits within a broader trend of abusive targeting and attacks against civil society in El Salvador.

Especially troubling, however, is the pattern of targeting of independent Salvadoran media that this joint investigation has uncovered.

Pegasus and the Media

Media organizations and individual journalists are now a regular target of hacking for NSO Group's government clients. A free and independent press is a threat to autocratic

rule and many of NSO Group's government clients are illiberal regimes. The voluminous hacking of Salvadoran media organizations and journalists is shocking but should come as no surprise.

Only a little over a year ago, we discovered government operatives used NSO Group's Pegasus spyware to hack 36 personal phones belonging to journalists, producers, anchors, and executives at the news organization *Al Jazeera*. The Citizen Lab and Amnesty International have also documented numerous other cases where journalists' phones were hacked with Pegasus, including *the New York Times*' Ben Hubbard, Sevinc Vaqifqizi, a freelance journalist for independent media outlet *Meydan TV*, Siddharth Varadarajan and MK Venu, co-founders of India's the *Wire*, Dániel Németh, a photojournalist working out of Budapest, and numerous others. According to investigations undertaken as part of the Pegasus Project, at least 180 journalists were selected as targets for potential Pegasus hacking.

Further highlighting the consistent threat posed by Pegasus to journalists, Daniel Lizárraga—a journalist whose phone we confirmed was hacked with Pegasus in this case—was also targeted in 2016 by the Mexican Pegasus operator while in a previous role at a Mexican NGO. Given the lack of due diligence and proper regulations, it should come as no surprise that individual victims of Pegasus hacking may have been targeted by multiple NSO Group clients over time, as Lizárraga's case illustrates.

The lesson from this case is obvious: an unregulated spyware marketplace is a grave threat to media worldwide, and to civil society.

Appendix A: Hacking Timeline

The following table of dates of successful hacking *excludes* dates of attempted but unsuccessful hacking. This table is *not* intended to be a comprehensive inventory of every date that the spyware was active on a phone. Each entry represents a separate instance where NSO's exploits were fired at a phone resulting in successful infection.

Several factors can influence the number of times infections happen. For example, if a target is selected for persistent surveillance, the exploit may be fired more often if the user frequently reboots their phone, as modern versions of the Pegasus spyware are believed to feature persistence via re-exploitation. If the target does not reboot their phone, the spyware may run for some time without the exploit being fired again.

Individual	Organization	Dates of Successful Hacking
Noah Bullock	Cristosal	1. On or around 2021-09-04
		2. On or around 2021-09-28
		3. On or around 2021-11-12

Individual	Organization	Dates of Successful Hacking
(Individual #1)	Diario El Mundo	1. On or around 2021-06-03
		2. On or around 2021-06-30
Ricardo Avelar	El Diario de Hoy	1. On or around 2020-08-31
		2. On or around 2020-09-22
		3. On or around 2021-02-21
		4. On or around 2021-03-16
		5. On or around 2021-03-26
		6. On or around 2021-04-27
		7. On or around 2021-06-15
		8. On or around 2021-07-14
		9. On or around 2021-09-04
		10. On or around 2021-09-12
Ana Beatriz Lazo	El Faro	1. On or around 2021-10-04
Carlos Dada	El Faro	1. Sometime 2020-07-08 – 2020-07-17
		2. Sometime 2020-07-17 – 2020-07-24
		3. Sometime 2020-07-24 – 2020-07-30
		4. On or around 2020-07-31
		5. Sometime 2020-08-01 – 2020-08-14
		6. Sometime 2020-09-08 – 2020-10-22
		7. Sometime 2021-01-06 – 2021-01-12
		8. Sometime 2021-01-12 – 2021-01-20
		9. Sometime 2021-02-13 – 2021-02-23
		10. Sometime 2021-03-31 – 2021-04-17
		11. Sometime 2021-04-18 – 2021-05-12
		12. Sometime 2021-05-26 – 2021-06-09

Individual	Organization	Dates of Successful Hacking
Carlos Ernesto Martínez D'aubuisson	El Faro	1. Sometime 2020-06-29 – 2020-07-22
		2. Sometime 2020-07-25 – 2020-08-06
		3. Sometime 2020-09-07 – 2020-09-10
		4. Sometime 2020-09-10 – 2020-09-18
		5. Sometime 2020-09-18 – 2020-10-10
		6. Sometime 2020-10-10 – 2020-11-05
		7. Sometime 2020-11-05 – 2020-11-10
		8. Sometime 2020-11-23 – 2020-12-02
		9. Sometime 2020-12-02 – 2020-12-21
		10. Sometime 2020-12-26 – 2021-01-21
		11. Sometime 2021-02-11 – 2021-02-16
		12. Sometime 2021-02-17 – 2021-02-19
		13. Sometime 2021-02-23 – 2021-03-08
		14. Sometime 2021-03-08 – 2021-03-11
		15. Sometime 2021-03-19 – 2021-03-23
		16. Sometime 2021-04-03 – 2021-04-12
		17. Sometime 2021-04-12 – 2021-04-27
		18. Sometime 2021-04-28 – 2021-05-06
		19. Sometime 2021-05-06 – 2021-05-27
		20. Sometime 2021-05-29 – 2021-06-02
		21. Sometime 2021-06-16 – 2021-06-22
		22. Sometime 2021-06-22 – 2021-06-24
		23. Sometime 2021-06-27 – 2021-07-02
		24. On or around 2021-07-08
		25. On or around 2021-08-31
		26. On or around 2021-09-15
		27. On or around 2021-10-07
		28. On or around 2021-10-21
Daniel Lizárraga	El Faro	1. On or around 2021-04-12
		2. On or around 2021-04-15
		3. On or around 2021-04-27
		4. On or around 2021-05-20
		5. On or around 2021-06-04
		6. On or around 2021-06-15
		7. On or around 2021-06-23
		8. On or around 2021-07-08
Daniel Reyes	El Faro	1. Sometime 2020-10-01 – 2020-10-10
		2. On or around 2021-11-04

Individual	Organization	Dates of Successful Hacking
Efren Lemus	El Faro	1. On or around 2021-04-23
		2. On or around 2021-04-26
		3. On or around 2021-04-30
		4. On or around 2021-05-20
		5. On or around 2021-06-01
		6. On or around 2021-06-08
		7. On or around 2021-06-18
		8. On or around 2021-07-10
		9. On or around 2021-09-17
		10. On or around 2021-09-25
Gabriel Labrador	El Faro	1. Sometime 2020-08-06 – 2020-09-07
		2. Sometime 2020-09-11 – 2020-10-30
		3. On or around 2021-03-25
		4. On or around 2021-04-01
		5. On or around 2021-04-06
		6. On or around 2021-04-09
		7. On or around 2021-04-12
		8. On or around 2021-04-14
		9. On or around 2021-04-16
		10. On or around 2021-05-05
		11. On or around 2021-05-07
		12. On or around 2021-05-13
		13. On or around 2021-05-17
		14. On or around 2021-06-01
		15. On or around 2021-08-31
		16. On or around 2021-09-12
		17. On or around 2021-10-06
		18. On or around 2021-10-23
		19. On or around 2021-11-04
		20. On or around 2021-11-11
Gabriela Cáceres	El Faro	1. On or around 2021-04-17
		2. On or around 2021-05-11
		3. On or around 2021-05-15
		4. On or around 2021-05-21
		5. On or around 2021-06-06
		6. On or around 2021-06-15
		7. On or around 2021-06-17
		8. On or around 2021-06-21
		9. On or around 2021-07-14
		10. On or around 2021-08-31
		11. On or around 2021-09-08
		12. On or around 2021-09-17
		13. On or around 2021-09-24

Individual	Organization	Dates of Successful Hacking
José Luis Sanz	El Faro	1. Sometime 2020-07-04 – 2020-07-09
		2. Sometime 2020-07-09 – 2020-07-14
		3. On or around 2020-07-16
		4. On or around 2020-09-10
		5. On or around 2020-09-23
		6. On or around 2020-11-14
		7. On or around 2020-11-21
		8. On or around 2020-11-28
		9. On or around 2020-12-03
		10. On or around 2020-12-07
		11. On or around 2020-12-10
		12. On or around 2020-12-16
		13. On or around 2020-12-19
Julia Gavarrete (Phone #1)	El Faro	1. On or around 2021-03-16
		2. On or around 2021-04-08
		3. On or around 2021-04-13
		4. On or around 2021-04-14
		5. On or around 2021-04-16
		6. On or around 2021-04-18
		7. On or around 2021-04-20
		8. On or around 2021-04-23
		9. On or around 2021-04-26
		10. On or around 2021-05-05
		11. On or around 2021-05-20
		12. Sometime 2021-05-30 – 2021-06-06
		13. On or around 2021-06-10
		14. On or around 2021-06-28
		15. On or around 2021-09-08
Julia Gavarrete (Phone #2)	El Faro	1. On or around 2021-02-23
		2. On or around 2021-09-09
		3. On or around 2021-09-27
María Luz Nóchez	El Faro	1. On or around 2021-02-17
		2. On or around 2021-05-21
		3. On or around 2021-06-09
Mauricio Ernesto Sandoval Soriano	El Faro	1. Sometime 2020-08-19 – 2020-10-20
		2. On or around 2021-07-02
		3. On or around 2021-07-06
		4. On or around 2021-10-01
Nelson Rauda	El Faro	1. Sometime 2021-04-30 – 2021-05-01
		2. On or around 2021-05-18
		3. On or around 2021-06-16
		4. Sometime 2021-06-18 – 2021-08-11
		5. On or around 2021-08-31
		6. On or around 2021-09-10

Individual	Organization	Dates of Successful Hacking
Óscar Martínez	El Faro	1. On or around 2020-07-15
		2. On or around 2020-07-21 – 2020-07-28
		3. On or around 2020-08-12
		4. On or around 2020-08-17
		5. On or around 2020-08-19
		6. On or around 2020-09-12
		7. On or around 2020-09-29
		8. On or around 2020-10-01
		9. On or around 2020-10-03
		10. On or around 2020-10-29
		11. On or around 2020-11-12
		12. On or around 2020-11-16
		13. On or around 2020-11-18
		14. On or around 2020-12-07
		15. On or around 2020-12-10
		16. On or around 2020-12-18
		17. On or around 2020-12-20
		18. On or around 2020-12-22
		19. On or around 2021-01-08
		20. On or around 2021-01-10
		21. On or around 2021-01-13
		22. On or around 2021-01-26
		23. On or around 2021-01-27
		24. On or around 2021-02-21
		25. On or around 2021-03-08
		26. On or around 2021-03-15
		27. On or around 2021-03-18
		28. On or around 2021-03-25
		29. On or around 2021-04-01
		30. On or around 2021-05-03
		31. On or around 2021-05-21
		32. On or around 2021-06-02
		33. On or around 2021-06-16
		34. On or around 2021-06-22
		35. On or around 2021-06-23
		36. On or around 2021-07-07
		37. On or around 2021-08-30
		38. On or around 2021-09-08
		39. On or around 2021-09-27
		40. On or around 2021-10-08
		41. On or around 2021-10-25
		42. On or around 2021-10-30
Rebeca Monge	El Faro	1. On or around 2021-10-07

Individual	Organization	Dates of Successful Hacking
Roman Gressier	El Faro	1. On or around 2021-05-17
		2. On or around 2021-05-21
		3. On or around 2021-06-21
		4. On or around 2021-06-23
Roxana Lazo	El Faro	1. On or around 2021-04-19
		2. On or around 2021-04-27
		3. On or around 2021-06-02
		4. On or around 2021-06-07
		5. On or around 2021-06-23
		6. On or around 2021-06-24
		7. On or around 2021-07-06
		8. On or around 2021-09-10
		9. On or around 2021-09-24
		10. On or around 2021-10-02
		11. On or around 2021-10-21
		12. On or around 2021-11-02
Sergio Arauz	El Faro	1. Sometime 2020-08-12 – 2020-08-19
		2. Sometime 2020-09-10 – 2020-09-11
		3. Sometime 2020-09-13 – 2020-09-14
		4. Sometime 2020-09-18 – 2020-09-22
		5. On or around 2021-05-07
		6. On or around 2021-06-02
		7. Sometime 2021-06-09 – 2021-06-10
		8. On or around 2021-06-11
		9. On or around 2021-06-17
		10. On or around 2021-06-24
		11. On or around 2021-06-25
		12. On or around 2021-07-02
		13. On or around 2021-07-09
		14. On or around 2021-10-21
Valeria Guzmán	El Faro	1. Sometime 2020-07-04 – 2020-07-14
		2. On or around 2021-09-03
		3. On or around 2021-09-29
		4. On or around 2021-10-12
		5. On or around 2021-10-25
		6. On or around 2021-11-04
		7. On or around 2021-11-11
		8. On or around 2021-11-19
Víctor Peña	El Faro	1. Sometime 2021-11-22 – 2021-11-23
(Individual #2)	El Faro	1. Sometime 2020-09-09 – 2020-09-16
		2. On or around 2021-09-30
		3. Sometime 2020-11-16 – 2020-11-26

Individual	Organization	Dates of Successful Hacking
(Individual #3)	El Faro	1. Sometime 2020-09-07 – 2020-10-17
		2. Sometime 2020-11-30 – 2021-01-16
		3. On or around 2021-05-21
Jose Marinero	Fundación DTJ	1. On or around 2021-04-08
		2. On or around 2021-09-12
Xenia Hernandez	Fundación DTJ	1. On or around 2021-02-23
		2. On or around 2021-03-17
		3. On or around 2021-04-29
		4. On or around 2021-05-01
		5. On or around 2021-05-04
		6. Sometime 2021-05-04 – 2021-05-07
		7. On or around 2021-05-07
		8. On or around 2021-05-11
		9. On or around 2021-05-17
		10. On or around 2021-05-21
		11. On or around 2021-06-02
		12. On or around 2021-06-13
		13. On or around 2021-06-15
		14. On or around 2021-06-28
		15. On or around 2021-06-30
		16. On or around 2021-11-09
		17. On or around 2021-11-16
Beatriz Benitez	GatoEncerrado	1. On or around 2021-07-01
Ezequiel Barrera	GatoEncerrado	1. Sometime 2020-09-10 – 2020-09-11
		2. Sometime 2021-04-06 – 2021-04-11
		3. Sometime 2021-04-13 – 2021-04-16
		4. Sometime 2021-04-23 – 2021-04-25
		5. On or around 2021-06-07
		6. On or around 2021-06-21
		7. On or around 2021-06-30
		8. On or around 2021-07-08
		9. On or around 2021-09-19
Xenia Oliva (Phone #1)	GatoEncerrado	1. Sometime 2020-11-12 – 2020-11-25
		2. Sometime 2021-02-17 – 2021-02-26
		3. Sometime 2021-02-28 – 2021-03-09
		4. On or around 2021-04-08
		5. On or around 2021-05-21
Xenia Oliva (Phone #2)	GatoEncerrado	1. On or around 2021-10-26
		2. On or around 2021-11-04
(Individual #4)	La Prensa Gráfica	1. On or around 2021-09-27
Oscar Luna	Revista Digital Disruptiva	1. On or around 2021-04-18
		2. On or around 2021-09-29
(Individual #5)	(NGO #1)	1. On or around 2021-05-21

Individual	Organization	Dates of Successful Hacking
Mariana Belloso	(Independent Journalist)	1. On or around 2021-09-29
		2. On or around 2021-10-09
Carmen Tatiana Marroquín	(Economist and Columnist for Independent Media)	1. On or around 2021-09-05

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF Northern District of California

Form 1. Notice of Appeal from a Judgment or Order of a United States District Court

U.S. District Court case number: 3:22-cv-07513

Notice is hereby given that the appellant(s) listed below hereby appeal(s) to the United States Court of Appeals for the Ninth Circuit.

Date case was first filed in U.S. District Court: 11/30/2022

Date of judgment or order you are appealing: 03/08/2024

Docket entry number of judgment or order you are appealing: 78, 79

Fee paid for appeal? *(appeal fees are paid at the U.S. District Court)*

◉ Yes ○ No ○ IFP was granted by U.S. District Court

List all Appellants *(List **each** party filing the appeal. Do not use "et al." or other abbreviations.)*

Daniel Lizárraga

Is this a cross-appeal? ○ Yes ◉ No

If yes, what is the first appeal case number?

Was there a previous appeal in this case? ◉ Yes ○ No

If yes, what is the prior appeal case number? 24-2179

Your mailing address (if pro se):

City: State: Zip Code:

Prisoner Inmate or A Number (if applicable):

Signature /s/ Caroline DeCell **Date** 05/29/2024

Complete and file with the attached representation statement in the U.S. District Court

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 6. Representation Statement

Instructions for this form: http://www.ca9.uscourts.gov/forms/form06instructions.pdf

Appellant(s) *(List **each** party filing the appeal, do not use "et al." or other abbreviations.)*

Name(s) of party/parties:

Daniel Lizárraga

Name(s) of counsel (if any):

Carrie DeCell, Stephanie Krent, Jameel Jaffer, and Alex Abdo

Address: 475 Riverside Drive, Suite 302 New York, NY 10115

Telephone number(s): 646-745-8500

Email(s): carrie.decell@knightcolumbia.org

Is counsel registered for Electronic Filing in the 9th Circuit? ◉ Yes ○ No

---

Appellee(s) *(List only the names of parties and counsel who will oppose you on appeal. List separately represented parties separately.)*

Name(s) of party/parties:

NSO Group Technologies Limited
Q Cyber Technologies Limited

Name(s) of counsel (if any):

Joseph N. Akrotirianakis and Aaron S. Craig

Address: 633 West Fifth Street, Suite 1700, Los Angeles, CA 90071

Telephone number(s): 213-443-4355

Email(s): jakro@kslaw.com, acraig@kslaw.com

To list additional parties and/or counsel, use next page.

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

Continued list of parties and counsel: *(attach additional pages as necessary)*

Appellants

Name(s) of party/parties:

Name(s) of counsel (if any):

Address:

Telephone number(s):

Email(s):

Is counsel registered for Electronic Filing in the 9th Circuit? ○ Yes ○ No

Appellees

Name(s) of party/parties:

Name(s) of counsel (if any):

Address:

Telephone number(s):

Email(s):

Name(s) of party/parties:

Name(s) of counsel (if any):

Address:

Telephone number(s):

Email(s):

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF Northern District of California

Form 1. Notice of Appeal from a Judgment or Order of a United States District Court

U.S. District Court case number: 3:22-cv-07513

Notice is hereby given that the appellant(s) listed below hereby appeal(s) to the United States Court of Appeals for the Ninth Circuit.

Date case was first filed in U.S. District Court: 11/30/2022

Date of judgment or order you are appealing: 03/08/2024

Docket entry number of judgment or order you are appealing: 78, 79

Fee paid for appeal? *(appeal fees are paid at the U.S. District Court)*

◉ Yes ○ No ○ IFP was granted by U.S. District Court

List all Appellants *(List **each** party filing the appeal. Do not use "et al." or other abbreviations.)*

Carlos Dada, Sergio Arauz, Gabriela Cáceres Gutiérrez, Julia Gavarrete, Roman Gressier, Gabriel Labrador, Ana Beatriz Lazo Escobar, Efren Lemus, Carlos López Salamanca, Carlos Martínez, Óscar Martínez, María Luz Nóchez, Víctor Peña, Nelson Rauda Zablah, Daniel Reyes Martínez (continued)

Is this a cross-appeal? ○ Yes ◉ No

If yes, what is the first appeal case number?

Was there a previous appeal in this case? ○ Yes ◉ No

If yes, what is the prior appeal case number?

Your mailing address (if pro se):

City: State: Zip Code:

Prisoner Inmate or A Number (if applicable):

Signature /s Caroline DeCell **Date** 04/08/2024

Complete and file with the attached representation statement in the U.S. District Court

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 6. Representation Statement

Instructions for this form: http://www.ca9.uscourts.gov/forms/form06instructions.pdf

Appellant(s) *(List **each** party filing the appeal, do not use "et al." or other abbreviations.)*

Name(s) of party/parties:

Carlos Dada, Sergio Arauz, Gabriela Cáceres Gutiérrez, Julia Gavarrete, Roman Gressier, Gabriel Labrador, Ana Beatriz Lazo Escobar, Efren Lemus, Carlos López Salamanca, Carlos Martínez, Óscar Martínez, María Luz Nóchez, Víctor Peña, Nelson Rauda Zablah, Daniel Reyes Martínez, Mauricio Sandoval Soriano, and José Luis Sanz

Name(s) of counsel (if any):

Carrie DeCell, Stephanie Krent, Jameel Jaffer, and Alex Abdo

Address: 475 Riverside Drive, Suite 302 New York, NY 10115

Telephone number(s): 646-745-8500

Email(s): carrie.decell@knightcolumbia.org

Is counsel registered for Electronic Filing in the 9th Circuit? ◉ Yes ○ No

---

Appellee(s) *(List only the names of parties and counsel who will oppose you on appeal. List separately represented parties separately.)*

Name(s) of party/parties:

NSO Group Technologies Limited
Q Cyber Technologies Limited

Name(s) of counsel (if any):

Joseph N. Akrotirianakis and Aaron S. Craig

Address: 633 West Fifth Street, Suite 1700, Los Angeles, CA 90071

Telephone number(s): 213-443-4355

Email(s): jakro@kslaw.com, acraig@kslaw.com

To list additional parties and/or counsel, use next page.

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

Continued list of parties and counsel: *(attach additional pages as necessary)*

Appellants

Name(s) of party/parties:

Mauricio Sandoval Soriano, and José Luis Sanz.

Name(s) of counsel (if any):

Address:

Telephone number(s):

Email(s):

Is counsel registered for Electronic Filing in the 9th Circuit? ○ Yes ○ No

Appellees

Name(s) of party/parties:

Name(s) of counsel (if any):

Address:

Telephone number(s):

Email(s):

Name(s) of party/parties:

Name(s) of counsel (if any):

Address:

Telephone number(s):

Email(s):

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov

ADRMOP,APPEAL,CLOSED,RELATE

U.S. District Court
California Northern District (San Francisco)
CIVIL DOCKET FOR CASE #: 3:22-cv-07513-JD

Dada et al v. NSO Group Technologies Limited et al
Assigned to: Judge James Donato
Relate Case Case: 3:21-cv-09078-JD
Case in other court: Ninth Circuit, 24-02179
Cause: 28:1331 Fed. Question

Date Filed: 11/30/2022
Date Terminated: 03/08/2024
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory Actions
Jurisdiction: Federal Question

Plaintiff

Carlos Dada

represented by **Caroline DeCell**
Knight First Amendment Institute at Columbia University
475 Riverside Drive
Suite 302
New York, NY 10115
646-745-8500
Email: carrie.decell@knightcolumbia.org
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
Knight First Amendment Institute at Columbia University
475 Riverside Drive
Ste 302
New York, NY 10115
646-745-8502
Email: alex.abdo@knightcolumbia.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
Knight First Amendment Institute at Columbia University
475 Riverside Drive
Suite 302
New York, NY 10115
646-745-8500
Email: evan.welberfalcon@knightcolumbia.org
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer

Knight First Amendment Institute at
Columbia University
475 Riverside Drive
Suite 302
New York, NY 10115
646-745-8500
Email: jameel.jaffer@knightcolumbia.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
Knight First Amendment Institute at
Columbia University
475 Riverside Drive
Suite 302
New York, NY 10115
646-745-8511
Email: stephanie.krent@knightcolumbia.org
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
Schonbrun Seplow Harris Hoffman &
Zeldes LLP
200 Pier Ave.
Ste 226
Hermosa Beach, CA 90254
310-717-7373
Fax: 310-399-7040
Email: hoffpaul@aol.com
ATTORNEY TO BE NOTICED

Plaintiff

Sergio Arauz represented by

Caroline DeCell
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Gabriela Caceres Gutierrez represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Julia Gavarrete represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)

TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Roman Gressier represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Gabriel Labrador represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Ana Beatriz Lazo Escobar represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman

(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Efren Lemus represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Carlos Martinez represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE

ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Oscar Martinez represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Maria Luz Nochez represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Victor Pena represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Nelson Rauda Zablah represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY

PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Maurricio Sandoval Soriano represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Jose Luis Sanz represented by **Caroline DeCell**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Evan Daniel Welber Falcon
(See above for address)
TERMINATED: 09/01/2023
PRO HAC VICE

Jameel Jaffer
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Stephanie Krent
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Paul L. Hoffman
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Daniel Reyes Martinez represented by **Stephanie Krent**
(See above for address)
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
ATTORNEY TO BE NOTICED

Caroline DeCell
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Daniel Lizarraga represented by **Stephanie Krent**
(See above for address)
ATTORNEY TO BE NOTICED

Alexander A Abdo

(See above for address)
ATTORNEY TO BE NOTICED

Caroline DeCell
(See above for address)
ATTORNEY TO BE NOTICED

Plaintiff

Carlos Lopez Salamanca represented by **Stephanie Krent**
(See above for address)
ATTORNEY TO BE NOTICED

Alexander A Abdo
(See above for address)
ATTORNEY TO BE NOTICED

Caroline DeCell
(See above for address)
ATTORNEY TO BE NOTICED

V.

Defendant

NSO Group Technologies Limited represented by **Joseph N. Akrotirianakis**
King & Spalding LLP
633 West Fifth Street, Suite 1600
Los Angeles, CA 90071
(213) 443-4355
Fax: (213) 443-4310
Email: jakro@kslaw.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Aaron S Craig
KING & SPALDING LLP
633 WEST 5TH STREET
SUITE 1700
Los Angeles, CA 90071
310-443-4311
Fax: 310-443-4310
Email: acraig@kslaw.com
ATTORNEY TO BE NOTICED

Defendant

Q Cyber Technologies Limited represented by **Joseph N. Akrotirianakis**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Aaron S Craig
(See above for address)
ATTORNEY TO BE NOTICED

Amicus

Legal Scholars

represented by **Jennifer Dale Bennett**
Gupta Wessler LLP
505 Montgomery Street
Suite 625
San Francisco, CA 94111
415-573-0336
Email: jennifer@guptawessler.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jonathan Ellis Taylor
Gupta Wessler LLP
2001 K Street NW
Suite 850 North
Washington, DC 20006
202-888-1741
Email: jon@guptawessler.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Date Filed	#	Docket Text
11/30/2022	1	COMPLAINT (with jury demand) against All Defendants (Filing fee $402, receipt number ACANDC-17769136). Filed by Maria Luz Nochez, Ana Beatriz Lazo Escobar, Sergio Arauz, Carlos Dada, Nelson Rauda Zablah, Gabriel Labrador, Gabriela Caceres Gutierrez, Carlos Martinez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Efren Lemus, Julia Gavarrete, Oscar Martinez, Roman Gressier. (Attachments: # 1 Exhibit)(Hoffman, Paul) (Filed on 11/30/2022) Modified on 11/30/2022 (cjl, COURT STAFF). (Entered: 11/30/2022)
11/30/2022	2	Proposed Summons. (Hoffman, Paul) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	3	**CLERK'S NOTICE.** Completed Civil Cover Sheet Missing. Please complete Civil Cover Sheet JS-CAND 44 (Rev. 10/2020) and file as a separate docket entry.. *(This is a text-only entry generated by the court. There is no document associated with this entry.)* (bw, COURT STAFF) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	4	Civil Cover Sheet by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah . (Hoffman, Paul) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	5	This case will be randomly reassigned to a District Judge outside the San Jose Division pursuant to the Caseload Rebalancing Pilot Program approved by the Court effective March 1, 2018. For information, visit our web page at https://cand.uscourts.gov/notices/northern-district-extends-caseload-rebalancing-pilot-program/. (bw, COURT STAFF) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	6	Case reassigned to Judge William Alsup. The assigned judge participates in the Cameras in the Courtroom Pilot Project. See General Order No. 65 and http://cand.uscourts.gov/cameras. Caseload Rebalancing Judge no longer assigned to the case. Reassignment Order signed by Clerk (Attachments: # 1 Notice of Eligibility for Video Recording) (bw, COURT STAFF) (Filed on 11/30/2022) (Entered: 11/30/2022)

11/30/2022	7	MOTION for leave to appear in Pro Hac Vice *of Carrie DeCell* (Filing fee $ 317, receipt number ACANDC-17770244.) filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (DeCell, Caroline) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	8	MOTION for leave to appear in Pro Hac Vice *of Alexander Abdo* (Filing fee $ 317, receipt number ACANDC-17770410.) filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Abdo, Alexander) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	9	MOTION for leave to appear in Pro Hac Vice *of Stephanie Krent* (Filing fee $ 317, receipt number ACANDC-17770509.) filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Krent, Stephanie) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	10	MOTION for leave to appear in Pro Hac Vice *of Evan Welber Falcon* (Filing fee $ 317, receipt number ACANDC-17770591.) filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Welber Falcon, Evan) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	11	Summons Issued as to NSO Group Technologies Limited, Q Cyber Technologies Limited. (cjl, COURT STAFF) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	12	**Initial Case Management Scheduling Order with ADR Deadlines: Notice: The assigned judge participates in the Cameras in the Courtroom Pilot Project. See General Order No. 65 and http://cand.uscourts.gov/cameras. Case Management Statement due by 3/2/2023. Initial Case Management Conference set for 3/9/2023 11:00 AM in San Francisco, Courtroom 12, 19th Floor. (Attachments: # 1 Notice of Eligibility for Video Recording)(cjl, COURT STAFF) (Filed on 11/30/2022) (Entered: 11/30/2022)**
11/30/2022	13	Certificate of Interested Entities by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah (Hoffman, Paul) (Filed on 11/30/2022) (Entered: 11/30/2022)
11/30/2022	14	MOTION for leave to appear in Pro Hac Vice *of Jameel Jaffer* (Filing fee $ 317, receipt number ACANDC-17771770.) filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Jaffer, Jameel) (Filed on 11/30/2022) (Entered: 11/30/2022)
12/02/2022	15	ADMINISTRATIVE MOTION TO CONSIDER WHETHER CASES SHOULD BE RELATED PURSUANT TO LOCAL RULES 3-12 AND 7-11 filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson

		Rauda Zablah. Responses due by 12/6/2022. (Attachments: # 1 Exhibit, # 2 Exhibit, # 3 Declaration, # 4 Proposed Order)(Hoffman, Paul) (Filed on 12/2/2022) (Entered: 12/02/2022)
12/07/2022	16	MOTION for leave to appear in Pro Hac Vice *of Carrie DeCell* (Filing fee $ 317, receipt number ACANDC-17770244.) Filing fee previously paid on 11/30/2022 filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (DeCell, Caroline) (Filed on 12/7/2022) (Entered: 12/07/2022)
12/07/2022	17	MOTION for leave to appear in Pro Hac Vice *of Alexander Abdo* (Filing fee $ 317, receipt number ACANDC-17770410.) Filing fee previously paid on 11/30/2022 filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Abdo, Alexander) (Filed on 12/7/2022) (Entered: 12/07/2022)
12/07/2022	18	MOTION for leave to appear in Pro Hac Vice *of Stephanie Krent* (Filing fee $ 317, receipt number ACANDC-17770509.) Filing fee previously paid on 11/30/2022 filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Krent, Stephanie) (Filed on 12/7/2022) (Entered: 12/07/2022)
12/07/2022	19	MOTION for leave to appear in Pro Hac Vice *of Evan Welber Falcon* (Filing fee $ 317, receipt number ACANDC-17770591.) Filing fee previously paid on 11/30/2022 filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Welber Falcon, Evan) (Filed on 12/7/2022) (Entered: 12/07/2022)
12/07/2022	20	MOTION for leave to appear in Pro Hac Vice *of Jameel Jaffer* (Filing fee $ 317, receipt number ACANDC-17771770.) Filing fee previously paid on 11/30/2022 filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Jaffer, Jameel) (Filed on 12/7/2022) (Entered: 12/07/2022)
12/10/2022	21	**ORDER by Judge William Alsup granting 16 Motion for Pro Hac Vice. (afm, COURT STAFF) (Filed on 12/10/2022) (Entered: 12/10/2022)**
12/10/2022	22	**ORDER by Judge William Alsup granting 17 Motion for Pro Hac Vice. (afm, COURT STAFF) (Filed on 12/10/2022) (Entered: 12/10/2022)**
12/10/2022	23	**ORDER by Judge William Alsup granting 18 Motion for Pro Hac Vice. (afm, COURT STAFF) (Filed on 12/10/2022) (Entered: 12/10/2022)**
12/10/2022	24	**ORDER by Judge William Alsup granting 19 Motion for Pro Hac Vice. (afm, COURT STAFF) (Filed on 12/10/2022) (Entered: 12/10/2022)**
12/10/2022	25	**ORDER by Judge William Alsup granting 20 Motion for Pro Hac Vice. (afm, COURT STAFF) (Filed on 12/10/2022) (Entered: 12/10/2022)**
12/12/2022	26	NOTICE of Appearance by Caroline DeCell (DeCell, Caroline) (Filed on 12/12/2022) (Entered: 12/12/2022)
12/12/2022	27	NOTICE of Appearance by Jameel Jaffer (Jaffer, Jameel) (Filed on 12/12/2022) (Entered:

		12/12/2022)
12/12/2022	28	NOTICE of Appearance by Alexander A Abdo (Abdo, Alexander) (Filed on 12/12/2022) (Entered: 12/12/2022)
12/12/2022	29	NOTICE of Appearance by Stephanie Krent (Krent, Stephanie) (Filed on 12/12/2022) (Entered: 12/12/2022)
12/12/2022	30	NOTICE of Appearance by Evan Daniel Welber Falcon (Welber Falcon, Evan) (Filed on 12/12/2022) (Entered: 12/12/2022)
12/16/2022	31	AMENDED COMPLAINT against NSO Group Technologies Limited, Q Cyber Technologies Limited. Filed byMaria Luz Nochez, Ana Beatriz Lazo Escobar, Sergio Arauz, Carlos Dada, Nelson Rauda Zablah, Gabriel Labrador, Gabriela Caceres Gutierrez, Carlos Martinez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Efren Lemus, Julia Gavarrete, Oscar Martinez, Roman Gressier, Daniel Reyes Martinez, Daniel Lizarraga, Carlos Lopez Salamanca. (Attachments: # 1 Exhibit A)(DeCell, Caroline) (Filed on 12/16/2022) (Entered: 12/16/2022)
12/16/2022	32	Proposed Summons. (DeCell, Caroline) (Filed on 12/16/2022) (Entered: 12/16/2022)
12/16/2022		Electronic filing error. Previously issued Summons, on 11/30/22, at docket entry 11 , must be returned as Unexecuted or Executed before a new Summons may be Issued. [err102] Thi s filing will not be processed by the clerks office. Re: 32 Proposed Summons filed by Carlos Dada, Roman Gressier, Jose Luis Sanz, Gabriela Caceres Gutierrez, Carlos Martinez, Gabriel Labrador, Nelson Rauda Zablah, Efren Lemus, Victor Pena, Julia Gavarrete, Maria Luz Nochez, Ana Beatriz Lazo Escobar, Oscar Martinez, Daniel Reyes Martinez, Maurricio Sandoval Soriano, Sergio Arauz, Carlos Lopez Salamanca, Daniel Lizarraga. (cjl, COURT STAFF) (Filed on 12/16/2022) (Entered: 12/16/2022)
12/21/2022	33	Summons Returned Unexecuted by Maria Luz Nochez, Ana Beatriz Lazo Escobar, Sergio Arauz, Daniel Lizarraga, Carlos Dada, Nelson Rauda Zablah, Gabriel Labrador, Carlos Lopez Salamanca, Gabriela Caceres Gutierrez, Carlos Martinez, Victor Pena, Jose Luis Sanz, Maurricio Sandoval Soriano, Efren Lemus, Julia Gavarrete, Daniel Reyes Martinez, Oscar Martinez, Roman Gressier as to NSO Group Technologies Limited, Q Cyber Technologies Limited. (Abdo, Alexander) (Filed on 12/21/2022) (Entered: 12/21/2022)
12/21/2022	34	Proposed Summons. (Krent, Stephanie) (Filed on 12/21/2022) (Entered: 12/21/2022)
12/22/2022	35	Summons Issued as to NSO Group Technologies Limited, Q Cyber Technologies Limited. (cjl, COURT STAFF) (Filed on 12/22/2022) (Entered: 12/22/2022)
01/06/2023	36	**ORDER by Judge James Donato granting 15 Administrative Motion to Relate Case. (lrc, COURT STAFF) (Filed on 1/6/2023) (Entered: 01/06/2023)**
01/06/2023	37	Case Reassigned to Judge James Donato. Judge William Alsup no longer assigned to the case. Notice: The assigned judge participates in the Cameras in the Courtroom Pilot Project. See General Order No. 65 and http://cand.uscourts.gov/cameras. (mbc, COURT STAFF) (Filed on 1/6/2023) (Entered: 01/06/2023)
03/21/2023	38	NOTICE of Appearance by Joseph N. Akrotirianakis (Akrotirianakis, Joseph) (Filed on 3/21/2023) (Entered: 03/21/2023)
03/21/2023	39	NOTICE of Appearance by Aaron S Craig (Craig, Aaron) (Filed on 3/21/2023) (Entered: 03/21/2023)
03/22/2023	40	STIPULATION WITH PROPOSED ORDER *concerning Defendants' response and briefing schedule on a responsive motion* filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Daniel Lizarraga, Carlos Lopez Salamanca, Carlos Martinez,

		Oscar Martinez, Maria Luz Nochez, Victor Pena, Daniel Reyes Martinez, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Attachments: # 1 Declaration of Carrie DeCell in Support)(DeCell, Caroline) (Filed on 3/22/2023) (Entered: 03/22/2023)
03/27/2023	41	**ORDER. For Dkt. No. 40, defendants' response to the amended complaint is due April 14, 2023. If the response is a Rule 12 motion, plaintiffs may file their opposition by May 19, 2023, and defendants may file a reply by June 2, 2023. The Court will set a hearing on the motion if warranted. Signed by Judge James Donato on 3/27/2023.** ***(This is a text-only entry generated by the court. There is no document associated with this entry.)*** **(jdlc3, COURT STAFF) (Filed on 3/27/2023) (Entered: 03/27/2023)**
04/14/2023	42	MOTION to Dismiss *First Amended Complaint [Fed. R. Civ. P. 12(B)(2), (B)(6), Forum Non Conveniens]* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. Motion Hearing set for 5/25/2023 10:00 AM in San Francisco, Courtroom 11, 19th Floor before Judge James Donato. Responses due by 4/28/2023. Replies due by 5/5/2023. (Attachments: # 1 Declaration of Roy Blecher, # 2 Declaration of Yaron Shohat, # 3 Exhibit A to Declaration of Yaron Shohat, # 4 Proposed Order)(Akrotirianakis, Joseph) (Filed on 4/14/2023) (Entered: 04/14/2023)
04/20/2023	43	CERTIFICATE OF SERVICE by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Daniel Lizarraga, Carlos Lopez Salamanca, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Daniel Reyes Martinez, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah (Attachments: # 1 Exhibit 1, # 2 Exhibit 2) (DeCell, Caroline) (Filed on 4/20/2023) (Entered: 04/20/2023)
04/20/2023	44	OBJECTIONS to re 42 MOTION to Dismiss *First Amended Complaint [Fed. R. Civ. P. 12(B)(2), (B)(6), Forum Non Conveniens]* by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Daniel Lizarraga, Carlos Lopez Salamanca, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Daniel Reyes Martinez, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (DeCell, Caroline) (Filed on 4/20/2023) (Entered: 04/20/2023)
04/20/2023	45	MOTION to Dismiss *[CORRECTED]* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. Motion Hearing set for 5/25/2023 10:00 AM in San Francisco, Courtroom 11, 19th Floor before Judge James Donato. Responses due by 5/4/2023. Replies due by 5/11/2023. (Attachments: # 1 Declaration of Roy Blecher, # 2 Declaration of Yaron Shohat, # 3 Exhibit A to Declaration of Yaron Shohat, # 4 Proposed Order)(Akrotirianakis, Joseph) (Filed on 4/20/2023) (Entered: 04/20/2023)
04/21/2023	46	MOTION to Dismiss *[CORRECTED]* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. Motion Hearing set for 5/25/2023 10:00 AM in San Francisco, Courtroom 11, 19th Floor before Judge James Donato. Responses due by 5/5/2023. Replies due by 5/12/2023. (Attachments: # 1 Declaration of Roy Blecher, # 2 Declaration of Yaron Shohat, # 3 Exhibit A to Declaration of Yaron Shohat, # 4 Proposed Order)(Akrotirianakis, Joseph) (Filed on 4/21/2023) (Entered: 04/21/2023)
04/21/2023	47	RESPONSE re 44 Objection,, *to Plaintiffs Objection and Request to Strike Motion to Dismiss* by NSO Group Technologies Limited, Q Cyber Technologies Limited. (Akrotirianakis, Joseph) (Filed on 4/21/2023) (Entered: 04/21/2023)
05/19/2023	48	OPPOSITION/RESPONSE (re 46 MOTION to Dismiss *[CORRECTED]*) filed bySergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Daniel Lizarraga, Carlos Lopez Salamanca, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Daniel

		Reyes Martinez, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (DeCell, Caroline) (Filed on 5/19/2023) (Entered: 05/19/2023)
05/19/2023	49	**ORDER. The Court stated in an earlier order that it would set a hearing on defendants' Rule 12 motion if warranted. *See* Dkt. No. 41. Consequently, the hearing set for May 25, 2023, is vacated. Signed by Judge James Donato on 5/19/2023. *(This is a text-only entry generated by the court. There is no document associated with this entry.)* (jdlc3, COURT STAFF) (Filed on 5/19/2023) (Entered: 05/19/2023)**
05/26/2023	50	NOTICE of Appearance by Jennifer Dale Bennett *as counsel for amici curiae Legal Scholars* (Bennett, Jennifer) (Filed on 5/26/2023) (Entered: 05/26/2023)
05/26/2023	51	MOTION for Leave to File *Brief of Amici Curiae in Support of Plaintiffs' Opposition to Defendants' Motion to Dismiss* filed by Legal Scholars. (Attachments: # 1 Amicus brief, # 2 Proposed Order)(Bennett, Jennifer) (Filed on 5/26/2023) (Entered: 05/26/2023)
05/30/2023	52	MOTION for leave to appear in Pro Hac Vice (Filing fee $ 317, receipt number ACANDC-18311551.) filed by Legal Scholars. (Attachments: # 1 Certificate of standing) (Taylor, Jonathan) (Filed on 5/30/2023) (Entered: 05/30/2023)
05/31/2023	53	**ORDER by Judge James Donato granting 52 Motion for Pro Hac Vice as to Jonathan Taylor. (lrc, COURT STAFF) (Filed on 5/31/2023) (Entered: 05/31/2023)**
06/02/2023	54	REPLY (re 46 MOTION to Dismiss *[CORRECTED]*) filed byNSO Group Technologies Limited, Q Cyber Technologies Limited. (Akrotirianakis, Joseph) (Filed on 6/2/2023) (Entered: 06/02/2023)
06/15/2023	55	**ORDER GRANTING 51 MOTION FOR LEAVE TO FILE AMICI BRIEF. Signed by Judge James Donato on 6/15/2023. (jdlc3, COURT STAFF) (Filed on 6/15/2023) (Entered: 06/15/2023)**
08/17/2023	56	First MOTION for Protective Order *Entry* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. Motion Hearing set for 9/28/2023 10:00 AM in San Francisco, Courtroom 11, 19th Floor before Judge James Donato. Responses due by 8/31/2023. Replies due by 9/7/2023. (Attachments: # 1 Declaration of Aaron Craig in Support of Motion for Entry, # 2 Exhibit A, # 3 Exhibit B, # 4 Proposed Order)(Craig, Aaron) (Filed on 8/17/2023) (Entered: 08/17/2023)
08/17/2023	57	First MOTION to Shorten Time *Unopposed* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. (Attachments: # 1 Proposed Order Granting Unopposed Motion Shortening Time)(Craig, Aaron) (Filed on 8/17/2023) (Entered: 08/17/2023)
08/22/2023	58	**ORDER. For Dkt. No. 57, plaintiffs may file their opposition to defendants' protective order motion, Dkt. No. 56, by August 25, 2023. Defendants may file their reply by August 28, 2023. The motion is suitable for decision without oral argument pursuant to Civil Local Rule 7-1(b). The hearing set for September 28, 2023, is vacated. Signed by Judge James Donato on 8/22/2023. *(This is a text-only entry generated by the court. There is no document associated with this entry.)* (jdlc3, COURT STAFF) (Filed on 8/22/2023) (Entered: 08/22/2023)**
08/25/2023	59	OPPOSITION/RESPONSE (re 56 First MOTION for Protective Order *Entry*) filed bySergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Daniel Lizarraga, Carlos Lopez Salamanca, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Daniel Reyes Martinez, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Attachments: # 1 Declaration of Carrie DeCell, # 2 Exhibit A to DeCell Declaration, # 3 Exhibit B to DeCell Declaration, # 4 Exhibit C to DeCell Declaration) (DeCell, Caroline) (Filed on 8/25/2023) (Entered: 08/25/2023)

08/28/2023	60	REPLY (re 56 First MOTION for Protective Order *Entry*) filed byNSO Group Technologies Limited, Q Cyber Technologies Limited. (Akrotirianakis, Joseph) (Filed on 8/28/2023) (Entered: 08/28/2023)
09/01/2023	61	NOTICE of Change In Counsel by Evan Daniel Welber Falcon (Welber Falcon, Evan) (Filed on 9/1/2023) (Entered: 09/01/2023)
10/03/2023	62	**ORDER. For Dkt. No. 56, in the absence of an agreement by the parties on a protective order, the Court will enter the District's Stipulated Protective Order for Standard Litigation, which is available on the District website. The parties are directed to file by October 16, 2023, a proposed protective order consistent with this Order. Signed by Judge James Donato on 10/3/2023.** ***(This is a text-only entry generated by the court. There is no document associated with this entry.)*** **(jdlc3, COURT STAFF) (Filed on 10/3/2023) (Entered: 10/03/2023)**
10/16/2023	63	STIPULATION WITH PROPOSED ORDER *[In Support of Proposed Limited Protective Order]* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. (Attachments: # 1 [Proposed] Limited Protective Order)(Akrotirianakis, Joseph) (Filed on 10/16/2023) (Entered: 10/16/2023)
10/17/2023	64	**ORDER. The parties' proposed limited protective order, Dkt. No. 63, is denied. The parties were previously directed to file the Stipulated Protective Order for Standard Litigation in light of their prior disagreement on a protective order. Dkt. Nos. 56, 59, 62. The parties are directed to file a proposed protective order consistent with Dkt. No. 62. Signed by Judge James Donato on 10/17/2023.** ***(This is a text-only entry generated by the court. There is no document associated with this entry.)*** **(jdlc3, COURT STAFF) (Filed on 10/17/2023) (Entered: 10/17/2023)**
10/24/2023	65	STIPULATION WITH PROPOSED ORDER *REGARDING ENTERING [PROPOSED] PROTECTIVE ORDER* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. (Attachments: # 1 Proposed Order)(Craig, Aaron) (Filed on 10/24/2023) (Entered: 10/24/2023)
10/31/2023	66	**ORDER ENTERING PROTECTIVE ORDER. Signed by Judge James Donato on 10/31/2023. (jdlc3, COURT STAFF) (Filed on 10/31/2023) (Entered: 10/31/2023)**
11/14/2023	67	STIPULATION WITH PROPOSED ORDER *to Supplement Protective Order* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. (Attachments: # 1 Proposed Order Proposed Protective Order)(Craig, Aaron) (Filed on 11/14/2023) (Entered: 11/14/2023)
11/17/2023	68	**ORDER. The parties' request to supplement the protective order, Dkt. No. 67-1, is granted. Signed by Judge James Donato on 11/17/2023.** ***(This is a text-only entry generated by the court. There is no document associated with this entry.)*** **(jdlc3, COURT STAFF) (Filed on 11/17/2023) (Entered: 11/17/2023)**
11/20/2023	69	Statement *of Recent Decision pursuant to Civil Local Rule 7-3(d)(2)* by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Daniel Lizarraga, Carlos Lopez Salamanca, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Daniel Reyes Martinez, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. (Attachments: # 1 Exhibit A)(DeCell, Caroline) (Filed on 11/20/2023) (Entered: 11/20/2023)
12/05/2023	70	Administrative Motion to File Under Seal filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. (Attachments: # 1 Declaration of Aaron S. Craig - Unredacted Version, # 2 Exhibit A - Unredacted Version, # 3 Exhibit B - Unredacted Version, # 4 Exhibit C - Unredacted Version, # 5 Exhibit D - Unredacted Version, # 6

		Exhibit E - Unredacted Version, # 7 Exhibit F - Unredacted Version, # 8 Exhibit G - Unredacted Version, # 9 Declaration of Aaron S. Craig - Redacted, # 10 Proposed Order) (Craig, Aaron) (Filed on 12/5/2023) (Entered: 12/05/2023)
12/05/2023	71	CERTIFICATE OF SERVICE by NSO Group Technologies Limited, Q Cyber Technologies Limited re 70 Administrative Motion to File Under Seal (Craig, Aaron) (Filed on 12/5/2023) (Entered: 12/05/2023)
12/20/2023	72	STATEMENT OF RECENT DECISION pursuant to Civil Local Rule 7-3.d filed byNSO Group Technologies Limited, Q Cyber Technologies Limited. (Attachments: # 1 Exhibit 1) (Akrotirianakis, Joseph) (Filed on 12/20/2023) (Entered: 12/20/2023)
01/06/2024	73	Administrative Motion to File Under Seal filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. (Attachments: # 1 Declaration of Aaron S. Craig - Unredacted Version, # 2 Exhibit 1 - Supplemental Memorandum in Support of Motion to Dismiss - Unredacted, # 3 Exhibit 2 - Supplemental Declaration of Roy Blecher (Exhibits A-D) - Unredacted, # 4 Exhibit 3 - Declaration of Joseph N. Akrotirianakis - Unredacted, # 5 Declaration of Aaron S. Craig - Redacted, # 6 Proposed Order)(Craig, Aaron) (Filed on 1/6/2024) (Entered: 01/06/2024)
01/06/2024	74	ADMINISTRATIVE MOTION re 46 MOTION to Dismiss *[CORRECTED]*, 42 MOTION to Dismiss *First Amended Complaint [Fed. R. Civ. P. 12(B)(2), (B)(6), Forum Non Conveniens]* filed by NSO Group Technologies Limited, Q Cyber Technologies Limited. Responses due by 1/10/2024. (Attachments: # 1 Exhibit 1- Supplemental Memorandum in Support of Motion to Dismiss [Redacted], # 2 Exhibit 2 - Declaration of Roy Blecher [Redacted], # 3 Exhibit 3 - Declaration of Joseph N. Akrotirianakis - Redacted, # 4 Proposed Order)(Akrotirianakis, Joseph) (Filed on 1/6/2024) (Entered: 01/06/2024)
01/06/2024	75	CERTIFICATE OF SERVICE by NSO Group Technologies Limited, Q Cyber Technologies Limited re 73 Administrative Motion to File Under Seal (Akrotirianakis, Joseph) (Filed on 1/6/2024) (Entered: 01/06/2024)
01/09/2024	76	**ORDER. Defendant NSO Group's request to file supplemental briefing on its motion to dismiss, Dkt. No 74, is denied. No further briefing will be accepted. Signed by Judge James Donato on 1/9/2024.** ***(This is a text-only entry generated by the court. There is no document associated with this entry.)*** **(jdlc3, COURT STAFF) (Filed on 1/9/2024) (Entered: 01/09/2024)**
02/09/2024	77	**ORDER RE MOTIONS TO SEAL. Signed by Judge James Donato on 2/9/2024. (jdlc3, COURT STAFF) (Filed on 2/9/2024) (Entered: 02/09/2024)**
03/08/2024	78	**ORDER RE MOTION TO DISMISS. Signed by Judge James Donato on 3/8/2024. (jdlc3, COURT STAFF) (Filed on 3/8/2024) (Entered: 03/08/2024)**
03/08/2024	79	**JUDGMENT. Signed by Judge James Donato on 3/8/2024. ***Civil Case Terminated. (jdlc3, COURT STAFF) (Filed on 3/8/2024) (Entered: 03/08/2024)**
04/08/2024	80	NOTICE OF APPEAL to the 9th Circuit Court of Appeals filed by Sergio Arauz, Carlos Dada, Ana Beatriz Lazo Escobar, Julia Gavarrete, Roman Gressier, Gabriela Caceres Gutierrez, Gabriel Labrador, Efren Lemus, Carlos Lopez Salamanca, Carlos Martinez, Oscar Martinez, Maria Luz Nochez, Victor Pena, Daniel Reyes Martinez, Jose Luis Sanz, Maurricio Sandoval Soriano, Nelson Rauda Zablah. Appeal of Order 78 , 79 . (Appeal fee of $605 receipt number ACANDC-19297602 paid.) (DeCell, Caroline) (Filed on 4/8/2024) Modified on 4/9/2024 linking entry to relaated documents (dhm, COURT STAFF). (Entered: 04/08/2024)
04/09/2024		Electronic filing error. Document not properly linked. [err102]Corrected by Clerk's Office. No further action is necessary. Re: 80 Notice of Appeal to the Ninth Circuit,, filed by

		Carlos Dada, Roman Gressier, Jose Luis Sanz, Gabriela Caceres Gutierrez, Carlos Martinez, Gabriel Labrador, Nelson Rauda Zablah, Efren Lemus, Victor Pena, Julia Gavarrete, Maria Luz Nochez, Ana Beatriz Lazo Escobar, Oscar Martinez, Daniel Reyes Martinez, Maurricio Sandoval Soriano, Sergio Arauz, Carlos Lopez Salamanca (dhm, COURT STAFF) (Filed on 4/9/2024) (Entered: 04/09/2024)
04/09/2024	81	USCA Case Number 24-2179 Ninth Circuit for 80 Notice of Appeal to the Ninth Circuit, filed by Carlos Dada, Roman Gressier, Jose Luis Sanz, Gabriela Caceres Gutierrez, Carlos Martinez, Gabriel Labrador, Nelson Rauda Zablah, Efren Lemus, Victor Pena, Julia Gavarrete, Maria Luz Nochez, Ana Beatriz Lazo Escobar, Oscar Martinez, Daniel Reyes Martinez, Maurricio Sandoval Soriano, Sergio Arauz, Carlos Lopez Salamanca ; Time Schedule Order. Mediation Questionnaire due (Appellant) 4/15/2024, Appeal Opening Brief (No Transcript Due) (Appellant) 5/20/2024, Appeal Answering Brief (No Transcript Due) (Appellee) 6/17/2024. All briefs shall be served and filed pursuant to FRAP 31 and 9th Cir. R. 31-2.1. Failure of the appellant(s) to comply with this briefing schedule will result in automatic dismissal of the appeal. (dhm, COURT STAFF) (Filed on 4/9/2024) (Entered: 04/10/2024)
05/08/2024	82	MOTION to Extend Time to File Notice of Appeal filed by Daniel Lizarraga. Motion Hearing set for 6/13/2024 10:00 AM in San Francisco, Courtroom 11, 19th Floor before Judge James Donato. Responses due by 5/22/2024. Replies due by 5/29/2024. (Attachments: # 1 Declaration, # 2 Proposed Order)(DeCell, Caroline) (Filed on 5/8/2024) (Entered: 05/08/2024)
05/28/2024	83	**ORDER. For Dkt. No. 82, plaintiff Daniel Lizárraga may file a notice of appeal by June 4, 2024. Fed. R. App. P. 4(a)(5)(A). Signed by Judge James Donato on 5/28/2024.** ***(This is a text-only entry generated by the court. There is no document associated with this entry.)*** **(jdlc3, COURT STAFF) (Filed on 5/28/2024) (Entered: 05/28/2024)**
05/29/2024	84	NOTICE OF APPEAL to the 9th Circuit Court of Appeals filed by Daniel Lizarraga. Appeal of Judgment, Terminated Case 79 , Order, Terminate Motions 78 (Pay.gov Agency Tracking ID ACANDC-19297602.) (DeCell, Caroline) (Filed on 5/29/2024) (Entered: 05/29/2024)

PACER Service Center

Transaction Receipt

06/03/2024 10:44:08

PACER Login:	reedcanaan	**Client Code:**	
Description:	Docket Report	**Search Criteria:**	3:22-cv-07513-JD
Billable Pages:	21	**Cost:**	2.10