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**
JAMEEL JAFFER**
ALEX ABDO**
STEPHANIE KRENT**
EVAN WELBER FALCÓN**
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**

***Application for Admission Pro Hac Vice To Be Filed*

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, CARLOS MARTÍNEZ, ÓSCAR MARTÍNEZ, MARÍA LUZ NÓCHEZ, VÍCTOR PEÑA, NELSON RAUDA ZABLAH, MAURICIO SANDOVAL SORIANO, and JOSÉ LUIS SANZ,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED and Q CYBER TECHNOLOGIES LIMITED,

Defendants.

Case No. _____

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 eleven 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 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 co-wrote an in-depth profile of the MS-13 gang for The New York Times. He lives in La Libertad, El Salvador.

23. 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.

24. 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.

25. 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.

26. 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 (APES), the Salvadoran journalists' association. He currently lives in New York City while pursuing a master's degree at Columbia Journalism School.

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

28. 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

29. 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.

30. 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.

31. 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. Omrie 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.

32. 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

33. 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.

34. 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.

35. 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.

36. 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.

37. 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.

38. Independent security researchers at the Citizen Lab, Access Now, and Amnesty International—all organizations that have conducted in-depth investigations of spyware attacks around the world—have concluded that Plaintiffs in this case were targeted through zero-click attacks directed at their iPhones. Investigations by these 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.

39. 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.

40. 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 Defendants used their 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.

41. 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.

42. In July 2021, Amnesty International 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

43. 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.

44. 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 the victims of Pegasus attacks directed by authoritarian or rights-abusing governments. For example, 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 researcher, 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.

45. 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.

46. 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.

47. 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."

48. 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.

49. 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 at the University of Toronto's Munk School of Global Affairs & Public Policy, 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

50. 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.

51. 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 to Defendants and their clients.

52. For example, beginning in June 2020, Defendants and their clients hacked the device of Plaintiff Carlos Martínez, an El Faro reporter, at least twenty-eight times, and his device was actively infected with Pegasus for at least 269 days. At the time, Mr. Martínez was the lead El Faro reporter investigating the secret negotiations between the Salvadoran government and the MS-13 gang. His device was still actively infected with Pegasus when he provided it to security researchers at the Citizen Lab for forensic analysis in November 2021.

53. In September 2020, when El Faro first published its reporting on the MS-13 negotiations, Defendants and their clients hacked the devices of nine El Faro employees, including Plaintiffs Carlos Dada, Sergio Arauz, Gabriel Labrador, Carlos Martínez, Óscar Martínez, Mauricio Sandoval Soriano, and José Luis Sanz.

The devices of El Faro's employees were infected with Pegasus for approximately 149 cumulative days that month.

54. At least one El Faro employee's device was actively infected with Pegasus every day in October 2020. The devices of at least four El Faro employees—Carlos Dada, Gabriel Labrador, Carlos Martínez, and Mauricio Sandoval Soriano—were actively infected for at least twenty days that month.

55. 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.

56. 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.

57. 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 appendix to the Citizen Lab report summarizing the attacks, incorporated herein and attached hereto as Exhibit A.

58. 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 and 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.

59. 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, and Óscar Martínez—initially submitted eleven devices used by El Faro employees for further analysis by the Citizen Lab and 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 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.

60. 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

61. 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 eleven of the devices targeted in the attacks against El Faro, including those used by Plaintiffs Sergio Arauz, Julia Gavarrete, Roman Gressier, Efren Lemus, Gabriel Labrador, 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.

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

63. 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. Active infections persisted on his device for at least 167 days.

64. 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.

65. 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.

66. **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.

67. 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. Active infections persisted on his device for at least twenty-eight days. The Citizen Lab confirmed that Defendants and their clients exfiltrated data from Mr. Arauz's device in the course of these attacks, but it could not identify which data was stolen.

68. 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.

69. 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 his own device for analysis.

70. **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.

71. 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.

72. 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.

73. 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 whose information may have been exposed to Defendants and their clients. She also purchased a new iPhone to protect her sources following the attacks.

74. **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.

75. 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. The Citizen Lab confirmed that Defendants and their clients exfiltrated data from Ms. Gavarrete's personal device in the course of these attacks, but it could not identify which data was stolen.

76. 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, 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.

77. 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 security researchers at 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 create back-ups of her devices for analysis by the Citizen Lab and Access Now.

78. **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.

79. 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 Defendants and their clients exfiltrated data from his device in the course of these attacks, but it could not identify which data was stolen.

80. 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.

81. 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.

82. **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.

83. 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. His device was infected with Pegasus twice between August and October 2020, and infections persisted on his device for most of that period. His device was infected at least eighteen more times between March and November 2021. Overall, his device was actively infected with Pegasus for approximately 101 days. The Citizen Lab confirmed that Defendants and their clients exfiltrated data from Mr. Labrador's device in the course of these attacks, but it could not identify which data was stolen.

84. 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.

85. 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.

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

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

88. 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.

89. 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 submitting a back-up of her device for forensic analysis.

90. **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.

91. 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 Defendants and their clients exfiltrated data from Mr. Lemus's device in the course of these attacks, but it could not identify which data was stolen.

92. 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.

93. 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 of 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 submit a back-up of his device for forensic analysis.

94. **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.

95. Defendants and their clients hacked Mr. Martínez's device, an iPhone 11 owned by El Faro, at least twenty-eight times between June and October 2021. Active infections persisted on his device for at least 269 days.

96. 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.

97. 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 and informing family, friends, and sources whose information may have been exposed to Defendants and their clients. He also purchased a new iPhone following the attacks.

98. **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.

99. 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. Active infections persisted on his device for at least forty-nine days. The Citizen Lab confirmed that Defendants and their clients exfiltrated data from Mr. Martínez's device in the course of these attacks, but it could not identify which data was stolen.

100. 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.

101. 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 phones that he used in the months after the attacks were confirmed.

102. **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.

103. 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 Defendants and their clients exfiltrated data from Ms. Nóchez's device in the course of the attacks, but it could not identify which data was stolen.

104. 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.

105. 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, creating and submitting a back-up of her device for forensic analysis, and attending additional meetings about digital security following the attacks.

106. **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.

107. 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.

108. 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.

109. 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 of the attacks and by notifying sources and contacts that their information had been exposed to Defendants and their clients.

110. **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.

111. 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. Active infections persisted on his device for at least sixty-two days, including three days when he visited the U.S. Embassy in San Salvador.

112. 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, Tik Tok, 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.

113. 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.

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

115. 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 Defendants and their clients exfiltrated data from Mr. Sandoval Soriano's device in the course of these attacks, but it could not identify which data was stolen.

116. 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.

117. 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 assisting with El Faro's investigation of 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.

118. **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.

119. 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 Defendants and their clients exfiltrated data from Mr. Sanz's device in the course of the attacks, but it could not identify which data was stolen.

120. 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.

121. 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.

122. 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

123. 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."

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

125. 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.

126. 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)

127. 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.

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

129. 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 contained on those devices and in the cloud-based accounts connected to those devices.

130. Although Pegasus attacks are designed to leave no trace, analysis by the Citizen Lab confirmed that Defendants and their clients obtained data from at least nine 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)

131. 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.

132. 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.

133. 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)

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

135. 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

136. 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.

137. 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 Defendants and their clients obtained data from at least nine 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.

138. 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.

139. 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.

140. 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.

141. 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.

142. 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.

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

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

Count III
Trespass to Chattels

145. 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.

146. 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.

147. 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.

148. 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

149. 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.

150. 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 a 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 Defendants and their clients exfiltrated data from at least nine 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.

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

152. 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: November 30, 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**
Jameel Jaffer**
Alex Abdo**
Stephanie Krent**
Evan Welber Falcón**
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, Carlos Martínez, Óscar Martínez, María Luz Nóchez, Víctor Peña, Nelson Rauda Zablah, Mauricio Sandoval Soriano, and José Luis Sanz

***Application for Admission Pro Hac Vice To Be Filed*