Nos. 24-2179, 24-3463

IN THE

United States Court of Appeals for the Ninth Circuit

CARLOS DADA, ET AL.,

Plaintiffs-Appellants,

v.

NSO GROUP TECHNOLOGIES LIMITED; Q CYBER TECHNOLOGIES LIMITED,

Defendants-Appellees.

DANIEL LIZARRAGA,

Plaintiff-Appellant,

CARLOS DADA, ET AL.,

Plaintiffs,

v.

NSO GROUP TECHNOLOGIES LIMITED; Q CYBER TECHNOLOGIES LIMITED,

Defendants-Appellees.

On Appeal from the United States District Court for the Northern District of California
No. 3:22-cv-07513-JD, Hon. James Donato

BRIEF FOR AMICI CURIAE MICROSOFT CORPORATION, GOOGLE LLC, GITHUB, INC., LINKEDIN CORPORATION, TREND MICRO, INC., AND BIG CLOUD CONSULTANTS, LLC IN SUPPORT OF PLAINTIFFS-APPELLANTS

David A. Simon
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
1440 New York Avenue, N.W.
Washington, D.C. 20005
(202) 371-7120
Counsel for Amicus Curiae Google LLC

Robert M. Loeb
ORRICK, HERRINGTON & SUTCLIFFE LLP
2100 Pennsylvania Avenue, NW
Washington, DC 20037
(202) 339-8400
Counsel for Amici Curiae Microsoft Corporation, GitHub, Inc., LinkedIn Corporation, Trend Micro, Inc., and Big Cloud Consultants, LLC

Additional Counsel Listed on Inside Cover

William E. Ridgway
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
320 S. Canal St.
Chicago, Illinois 60606
(312) 407-0449

Counsel for Amicus Curiae Google LLC

Rachael Jensen
ORRICK, HERRINGTON & SUTCLIFFE LLP
300 West 6th Street, Suite 1850
Austin, TX 78701
(512) 582-6950

Counsel for Amici Curiae Microsoft Corporation, GitHub, Inc., LinkedIn Corporation, Trend Micro, Inc., and Big Cloud Consultants, LLC

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, counsel hereby state the following:

Amicus Microsoft Corporation ("Microsoft") is a publicly held corporation. Microsoft does not have a parent corporation, and no publicly held corporation holds 10% or more of its stock.

Amicus Google LLC ("Google") is an indirect subsidiary of Alphabet Inc., a publicly held corporation. Alphabet Inc. does not have a parent corporation and no publicly held company owns 10% or more of its outstanding stock.

Amicus GitHub, Inc. ("GitHub") is a wholly owned subsidiary of Microsoft, a publicly held corporation. Microsoft does not have a parent corporation and no publicly held corporation holds 10% or more of its stock.

Amicus LinkedIn Corporation ("LinkedIn") is a wholly owned subsidiary of Microsoft. Microsoft does not have a parent corporation and no publicly held corporation holds 10% or more of its stock.

Amicus Trend Micro, Inc. ("Trend") is a publicly held corporation traded on the Tokyo Stock Exchange. Trend does not have a parent

corporation, and no publicly held corporation holds 10% or more of its stock.

Amicus Big Cloud Consultants, LLC is a privately held Limited Liability Partnership. Big Cloud Consultants does not have a parent corporation, and no publicly held corporation owns any of its stock.

GOOGLE LLC

/s/ David A. Simon
David A. Simon
Counsel for Amicus Curiae Google LLC

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/Robert M. Loeb
Robert M. Loeb
Counsel for Amici Curiae Microsoft Corporation, GitHub, Inc., LinkedIn Corporation, Trend Micro, Inc., and Big Cloud Consultants, LLC

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules and Regulations

Other Authorities

Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L.R. 1561 (2010) 21

Remarks by the President at the Cybersecurity and Consumer Protection Summit, The White House (Feb. 13, 2015), https://tinyurl.com/y36d8vdz 25, 26, 27

Response from NSO and governments, The Guardian (July 20, 2021), https://tinyurl.com/9z44chm7 7

Stephanie Kirchgaessner et al., *Revealed: Leak uncovers global abuse of cyber-surveillance weapon*, The Guardian (July 18, 2021), https://tinyurl.com/yp7speeb 5, 17, 20, 21

Stephanie Kirchgaessner, *White House issues warning to US firms interested in acquiring Israeli surveillance tech*, The Guardian (June 29, 2023), https://tinyurl.com/z3ehrxsp 19

U.S. Department of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://tinyurl.com/2d8vspwz 9, 20

U.S. Department of State, *The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://tinyurl.com/msz3k7tz 8

Vas Panagiotopoulos, *Notorious Spyware Maker NSO Group is Quietly Plotting a Comeback*, Wired (Jan. 24, 2024), https://tinyurl.com/3ps94rn8 19

INTEREST OF AMICI CURIAE[1]

Amici Microsoft Corporation, Google LLC, GitHub, Inc., LinkedIn Corporation, Trend Micro, Inc., and Big Cloud Consultants, LLC, all have strong interests in the issues raised by these appeals seeking to hold NSO Group Technologies Ltd. ("NSO") accountable for facilitating spyware attacks on the products and services of U.S. technology companies. Private-sector companies like NSO are investing heavily in creating cyber-surveillance tools and selling "cyber-surveillance as a service" to foreign governments and other customers. These spyware tools allow the user to covertly track someone's whereabouts, listen in on their conversations, read their texts and emails, look at their photographs, steal their contacts list, download their data, review their internet search history, and more. NSO designs its cyber-surveillance tools to evade detection by the user, the device being attacked (e.g., a phone or personal computer), as well as each and every application from which the spy tools covertly extract the user's personal and commercial

[1] No counsel for a party authored this brief in whole or in part. No party, counsel for a party, or any person other than amicus and their counsel made a monetary contribution intended to fund the preparation or submission of the brief. All parties consented to the filing of this brief.

information and movements. Foreign governments and criminal organizations use these NSO surveillance tools to spy on human rights activists, journalists, and others, including U.S. citizens.

Amici are leading technology companies in the United States. Their products and services are widely used by customers all over the world, making them targets for malicious actors such as NSO. *Amici* accordingly, engage in significant cybersecurity efforts to secure their technology from such malicious actors. One example is the international Cybersecurity Tech Accord (https://cybertechaccord.org/), comprised of over 100 companies, committed to protecting cyberspace from malicious actors. Members of the Tech Accord developed international standards seeking to restrict the commercial sale and use of spyware. As part of this Accord and otherwise, *amici* have committed to protecting users and customers—both private and governmental—from cyberattacks, and working collaboratively to enhance cybersecurity across the board. And through the Tech Accord and otherwise, the industry continues to shed light on the threat posed by NSO and similar actors.

Relatedly, *amici* invest billions of dollars every year on their own cybersecurity and the cybersecurity of governmental and private software and services. In 2021, Microsoft and Google, and other technology companies, partnered with the White House to address cybersecurity as a national imperative, announcing significant nationwide cybersecurity investments in partnership with the Administration.

Consistent with their focus on cybersecurity and protecting their customers from cyber-surveillance attacks, *amici* have a strong interest in ensuring that entities who facilitate covert access to their products and services in violation of federal and state law are held accountable in U.S. courts. Holding bad actors accountable is vital to deterring malicious cyber-surveillance and other cyber-attacks.

The United States and California, likewise, have fundamental interests in preventing the proliferation of such spyware tools that threaten national security and in protecting U.S. technology companies from hackers (both foreign and domestic) exploiting their products and services. Those strong interests are reflected in the Computer Fraud and Abuse Act and the California Comprehensive Computer Data

Access and Fraud Act, both of which make it illegal to access a computing device without proper authorization. *See* 18 U.S.C. § 1030; Cal. Penal Code § 502. As *amici* explain below, the deterrence provided by those laws plays a crucial role in protecting U.S. national security and the economic interests of the United Sates and California.

INTRODUCTION

In July 2021, Amnesty International and a French news organization called Forbidden Stories obtained a database of over 50,000 phone numbers believed to belong to individuals whose devices were targeted for hacking and covert surveillance using a powerful spyware program called Pegasus. *See* Stephanie Kirchgaessner et al., *Revealed: Leak uncovers global abuse of cyber-surveillance weapon*, The Guardian (July 18, 2021), https://tinyurl.com/yp7speeb. The database included phone numbers belonging to 14 heads of state—including the President of France, Emmanuel Macron; then-President of Iraq, Barham Salih; the King of Morocco, Mohammed VI; then-Prime Minister of Pakistan, Imran Khan; and the Prime Minister of Egypt, Mostafa Madbouly—600 government officials, over 180 journalists, hundreds of executives, religious leaders, and academics, as well as political dissidents and activists in over 45 countries. *See id.*; Devirupa Mitra, *Pegasus Project: 14 World Leaders in Leaked Database*, The Wire (July 21, 2021), https://tinyurl.com/y43n9x42. A collaborative investigation by 17 major media organizations found evidence of

successful or attempted Pegasus spyware infections in over half of the targeted devices examined.[2] *See* Kirchgaessner et al., *supra* at 5.

Defendant NSO is a foreign company that develops and sells spyware tools, including Pegasus, to clients all over the world. *See* David Pegg & Sam Cutler, *What is Pegasus spyware and how does it hack phones?*, The Guardian (July 18, 2021), https://tinyurl.com/fetmmp5p. NSO's Pegasus spying tools allow the user to hack into an Apple or Android device by exploiting what are known as "zero-day" vulnerabilities—vulnerabilities that are unknown to the developer such that it has had "zero days" to patch the unknown vulnerability. *See id.* Pegasus is particularly insidious because it can remotely infiltrate a device anywhere in the world, often without any intervention by the user whatsoever. *See id.* And once Pegasus accesses the device, it can be used to extract photos and text messages, record phone calls, monitor the device's location, and even remotely activate the device's microphone and camera. *See id.* It can remain

---

[2] The results for the other half of the devices were "inconclusive," in some cases because the targets replaced their handsets prior to testing, and in other cases because the devices did not log the kind of information required for the investigation to detect infiltration by Pegasus. *See id.*

undetected on a target's device for years, secretly collecting sensitive data. *See id.*

NSO admits to having sold Pegasus to approximately 40 different governments around the world. *See Response from NSO and governments*, The Guardian (July 20, 2021), https://tinyurl.com/9z44chm7. It claims to have extensive protections in place to prevent abuse of its spyware, including vetting its clients for human rights abuses, contractually limiting the use of its spyware to law enforcement and counter-terrorism efforts, and putting blocks in place to prevent infiltrating phones belonging to Americans. *Id.* But as evidenced by the leaked database's inclusion of targets with zero connection to criminality or terrorism, these protections—if they ever existed—have failed to prevent abuse. It appears that, once a government purchased Pegasus from NSO, it could use the tool to hack and spy on whomever it wanted.

In November 2021, a few months after reports surfaced regarding the leaked database, the United States added NSO to the Commerce

Department's "Entity List"—effectively, an economic blacklist[3]—for engaging in "activities contrary to the national security or foreign policy interests of the United States." Addition of Certain Entities to the Entity List, 15 C.F.R. § 744 (2021). Specifically, the Commerce Department declared that NSO acted contrary to U.S. national security and foreign policy interests by "develop[ing] and suppl[ying] spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers." *Id.* In a statement accompanying the decision, Commerce Secretary Gina Raimondo explained that "[t]he United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten the cybersecurity of members

---

[3] "The Entity List is a tool … to restrict the export, reexport, and in-country transfer of items … to persons (individuals, organizations, companies) reasonably believed to be involved, have been involved, or pose a significant risk of being or becoming involved, in activities contrary to the national security or foreign policy interests of the United States." U.S. Department of State, *The United States Adds Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://tinyurl.com/msz3k7tz; *see also* David E. Sanger et al., *U.S. Blacklists Israeli Firm NSO Group Over Spyware*, N.Y. Times (Nov. 3, 2021), https://tinyurl.com/62bjt4y5.

of civil society, dissidents, government officials, and organizations here and abroad." U.S. Department of Commerce, *Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities* (Nov. 3, 2021), https://tinyurl.com/2d8vspwz.

The New York Times called this "the strongest step an American president has taken to curb abuses in the global market for spyware." Sanger et al., *supra* at 8 n.3. Such a strong response was clearly warranted. NSO spread these dangerous spyware tools throughout the world, placing them in the hands of governments and individuals who had demonstrated a willingness to abuse them, including by attacking products and services sold by U.S. companies and devices possessed by U.S. citizens.

NSO's assurance that its powerful spying technology would never be used against Americans also turned out to be an empty promise. About a month after the United States added NSO to the Entity List, news media reported that iPhones belonging to nine employees of the U.S. Department of State were hacked using NSO's spyware tools. *See* Christopher Bing & Joseph Menn, *U.S. State Department phones hacked with Israeli company software*, Reuters (Dec. 3, 2021),

https://tinyurl.com/ykwdnyve; Lily Hay Newman, *NSO Group Spyware Hits at Least 9 US State Department Phones*, Wired (Dec. 3, 2021), https://tinyurl.com/4e929cbk. When asked for comment on these revelations, a spokesperson for the State Department simply "point[ed] to the Commerce Department's recent decision to place [NSO] on an entity list," Bing et al., *supra* at 9, essentially acknowledging the attack on U.S. government officials.

Even if NSO's spyware tools were not being used to target U.S. citizens and officials, the proliferation of these tools would still inflict substantial harm on important U.S. interests. These tools exploit the products and services sold by U.S. technology companies, harming the reliability of and user confidence in the technology sold. U.S. technology companies spend billions of dollars a year to defend against cybersecurity threats like these.

For all these reasons, both the United States and California have strong interests in deterring and preventing NSO and other such malicious actors from proliferating dangerous spyware that exploits the products and services of U.S. technology companies.

Plaintiffs in this case are pursuing an anti-hacking action, which, if successful, will help deter NSO and other similar actors. Plaintiffs are journalists for a publication in El Salvador, and they allege that one or more of NSO's clients hacked their devices using NSO's spyware. *See* First Am. Compl. at ¶¶ 1-7. They bring claims against NSO under both federal and state anti-hacking laws, including the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and the California Comprehensive Computer Data Access and Fraud Act, California Penal Code § 502. *Id.* at ¶¶ 137-66. The district court, however, dismissed Plaintiffs' claims under the doctrine of *forum non conveniens*. In so ruling, the court found that "Plaintiffs did not demonstrate *any* local interest or stake in the events alleged in the complaint." *Dada v. NSO Grp. Techs. Ltd.*, Case No. 3:22-cv-07513-JD, 2024 WL 1024736, at *4 (N.D. Cal. Mar. 8, 2024) (emphasis added). In making that finding, the district court shrugged off the United States's national security interest in preventing the proliferation of NSO's commercial spyware tools as a "massive generalization." *Id.* And the court afforded no weight to California's interest in protecting its technology companies, citing other lawsuits

against NSO in the district, and concluding that those lawsuits purportedly "protect[]" this interest enough. *Id.*

The district court erred in assigning no weight to the United States's and California's powerful interests implicated by this litigation. The United States has explicitly determined that NSO's sale of commercial spyware to foreign governments—the very conduct at issue in this case—is a threat to the United States's national security and foreign policy interests. And both the United States and California have demonstrated their interests in protecting domestic technology companies from foreign hackers by passing federal and state anti-hacking laws—the very laws under which Plaintiffs bring their claims here. Failure to acknowledge, let alone appropriately weigh these interests, is error. Accordingly, this Court should reverse the district court's dismissal of Plaintiffs' claims.

ARGUMENT

The United States And California Have Strong Interests In Deterring NSO's Sale Of Commercial Spyware.

The district court was required to adequately consider and reasonably weigh all of the public and private interest factors in its *forum non conveniens* analysis—including the United States's national

security interest and both the United States's and California's interests in protecting domestic technology companies from foreign hackers. In general, national security concerns "weigh heavily in favor of conducting international litigation in a U.S. rather than a foreign court." *U.S.O. Corp. v. Mizuho Holding Co.*, 547 F.3d 749, 755 (7th Cir. 2008). And that is especially true here, where the federal government has repeatedly expressed a national security interest specifically in NSO's conduct. Further, both the United States and California have powerful economic interests in protecting U.S. technology companies from spyware attacks on their products and services. The district court failed to properly consider these significant interests here.

A. The United States has a fundamental national security interest in deterring the sale and proliferation of NSO's spyware.

The United States has explicitly stated that the proliferation of spyware generally—and NSO's sale of Pegasus *specifically*—poses a substantial threat to national security.

In November 2021, the U.S. Department of Commerce essentially blacklisted NSO by adding it to the "Entity List" for "develop[ing] and suppl[ying] spyware to foreign governments that used this tool to

maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers." 15 C.F.R. § 744; Sanger et al., *supra* at 8 n.3. The Commerce Department stated without equivocation that NSO's sale of spyware to foreign governments constituted "activities contrary to the national security or foreign policy interests of the United States." 15 C.F.R. § 744.

The conduct underlying the government's determination that NSO's activities threaten national security is the *very conduct* at issue in this case. *See* Brief for the United States as Amicus Curiae at 15-16, *Apple v. NSO Grp. Techs. Ltd. v. WhatsApp Inc.*, (U.S. 2022) (No. 21-1338) (discussing the fact that NSO was determined a national security threat "for the very type of activities allegedly at issue in this case"—in a case regarding the proliferation of NSO's spyware and sales to foreign countries). Plaintiffs allege that NSO sold Pegasus to one or more clients who then used it to target Plaintiffs because they are journalists. First Am. Compl. ¶¶ 1-7. And the Commerce Department determined that this conduct—"develop[ing] and supply[ing] spyware to foreign governments that use this tool to maliciously target … journalists"—is "contrary to the national security or foreign policy interests of the

United States." 15 C.F.R. § 744. Thus, Plaintiffs are seeking to redress the very conduct by NSO that has been a significant concern of the U.S. government. *See id.*

The district court never mentioned the Commerce Department's determination. Nor did it acknowledge that NSO's repeated sale of powerful spyware tools to foreign governments has already resulted in its clients surveilling journalists, dissidents, heads of state, and even nine employees of the U.S. State Department. *See* Kirchgaessner et al., *supra* at 5; Mitra, *supra* at 5; Bing et al., *supra* at 9; Newman, *supra* at 10. Instead, the district court focused exclusively on the United States's interest in "managing the use of spyware," and dismissed that interest as "a massive generalization of no utility for the *forum non conveniens* analysis." *Dada*, 2024 WL 1024736, at *4. This was error—both because, as explained above, the United States has unequivocally articulated a national security interest in NSO's conduct underlying this case, and because the United States *does* have a powerful interest in preventing the proliferation of spyware.

The United States is part of an "international technology ecosystem" in which international standards and norms govern the use

of emerging technology. *See* Exec. Order No. 14093, 88 Fed. Reg. 18957, 18957 (Mar. 27, 2023). When foreign governments or other groups "use[] commercial spyware for improper purposes," such as to commit "human rights abuses or suppress[] … civil liberties," that misuse threatens the United States's "national security and foreign policy interests." *Id.* That is because the United States has a "core interest[]" in "upholding and advancing democracy," "human rights," and the "freedom and dignity" of "activists, dissidents, and journalists" around the world. *Id.* It is also the case because malicious actors in the international technology ecosystem undermine international standards and norms for the use of technology. *See id.* And a world in which the abuse of powerful spyware is widespread is a world in which the United States is not safe.

That is why, in March 2023, President Biden issued an Executive Order in which he explained that the United States has a "fundamental national security and foreign policy interest" in fostering an "international technology ecosystem that protects the integrity of international standards development; enables and promotes the free flow of data and ideas with trust; protects our security, privacy, and

human rights; and enhances our economic competitiveness." *Id.* The Order concluded that the "proliferation of commercial spyware" and its "misuse[] by foreign governments" is thus fundamentally at odds with the United States's national security interests. *Id.*; *see also* U.S. Dept. of Commerce, *supra* at 9 (explaining federal interest in deterring "malicious activities that threaten the cybersecurity of members of civil society, dissidents, government officials, and organizations *here and abroad*" (emphasis added)).

As the world learned in 2021, when news media released reports regarding the leaked database of Pegasus hacking targets, NSO's spyware is being used to target political opponents, silence dissent, engage in espionage against foreign nations, and more. *See, e.g.*, Kirchgaessner et al., *supra* at 5. What became abundantly clear from the leaked database was that once NSO gives a customer access to its powerful spyware tools, that customer can use them to target whomever it wants—including the United States. *See* Bing et al., *supra* at 9.

And even if NSO did try to limit its clients' use of Pegasus for legitimate law enforcement and national security purposes, its spyware can easily fall into the wrong hands. Spyware providers and customers

can themselves be the victims of a hack in which malicious actors steal their spyware tools. That is exactly what happened to the Italian company Hacking Team—one of NSO's competitors—in 2015. *See* Andy Greenberg, *Hacking Team Breach Shows a Global Spying Firm Run Amok*, Wired (July 6, 2015), https://tinyurl.com/y2u5shjj. Not only did the hacker expose some of Hacking Team's clients, but it also disclosed "the source code of the company's hacking tools." Lorenzo Franceschi-Bicchierai, *The Vigilante Who Hacked Hacking Team Explains How He Did It*, Vice (Apr. 15, 2016), https://tinyurl.com/y284rpou.

Additionally, the use of NSO's spy tools can also lead to further proliferation. The individuals or entities targeted for surveillance, if they discover the hacking attempt, can sometimes obtain the spyware tools themselves by reverse-engineering the technology. That is how human rights activist Ahmed Mansoor and cybersecurity laboratory Citizen Lab identified the "chain of zero-days exploits" a hacker wielding Pegasus attempted to use to hack into Mansoor's Apple device. *See* Bill Marczak & John Scott-Railton, The Citizen Lab, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE*

Human Rights Defender, at 5-6, 9-11 (Aug. 24, 2016), https://tinyurl.com/y3uvmlev.

The greater the proliferation of sophisticated, powerful spyware, the greater the risk of it falling into the wrong hands. For that reason, President Biden's March 2023 Executive Order largely prohibits federal agencies from using commercial spyware, thereby "ensur[ing] that the United States Government does not contribute, directly or indirectly, to the proliferation of commercial spyware that has been misused by foreign governments or facilitate such misuse." 88 Fed. Reg. at 18957; *see also* Vas Panagiotopoulos, *Notorious Spyware Maker NSO Group is Quietly Plotting a Comeback*, Wired (Jan. 24, 2024), https://tinyurl.com/3ps94rn8. And the national security concerns raised by the proliferation of NSO's spyware have caused the White House to issue warnings against transactions with NSO. *See* Stephanie Kirchgaessner, *White House issues warning to US firms interested in acquiring Israeli surveillance tech*, The Guardian (June 29, 2023), https://tinyurl.com/z3ehrxsp (warning against a proposed transaction as potentially posing a "counterintelligence threat to the US government"). As the National Security Council has explained, "the proliferation of

tools like those produced by NSO Group pose[s] a serious counterintelligence and security risk to US personnel and systems." *Id.*

NSO has reportedly made significant revenue by exploiting the products and services of U.S. technology companies.[4] Impediments and costs are necessary to deter NSO and other such actors from engaging in these profitable activities that threaten the United States's national security. For instance, the Commerce Department uses its export controls to deter doing business with NSO. *See* U.S. Dept. of Commerce, *supra* at 9 ("The United States is committed to aggressively using export controls to hold companies accountable that develop, traffic, or use technologies to conduct malicious activities that threaten" national security). Another key tool is providing causes of action to

---

[4] *See* Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, Wired (Apr. 17, 2015), https://tinyurl.com/yyyk6n5w; *see also* Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times (July 13, 2013), https://tinyurl.com/yypwwa8c (reporting that a single "zero-day exploit in Apple's iOS operating system sold for $500,000"); Mark Mazzetti et al., *A New Age of Warfare: How Internet Mercenaries Do Battle for Authoritarian Governments*, N.Y. Times (Mar. 21, 2019), https://tinyurl.com/y39pzhtc (NSO's first sale of Pegasus was to Mexico for $15 million, with an additional $77 million for NSO's surveillance management services).

those companies and customers subject to hacking facilitated by NSO, such as the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, under which Plaintiffs assert their claims here.

Congress initially enacted the CFAA to fulfill specific national security imperatives—criminalizing hacking into government computers or misusing a computer to obtain national security secrets or personal financial records. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L.R. 1561, 1563-64 (2010). And Congress has consistently expanded the CFAA to meet this important policy goal, making it "one of the most far-reaching criminal laws in the United States Code." *Id.* at 1561.

Through a series of amendments, Congress broadened the CFAA to apply to international hacking cases and provide victims with a cause of action under which to sue both foreign and domestic hackers. In 1994, Congress added a private right of action to the CFAA, enabling hacking victims to seek damages from hackers directly and imposing additional costs on hackers beyond criminal enforcement. *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001(d), 108 Stat. 1796, 2098 (1994). Congress then specifically

amended the CFAA to apply extraterritorially. In 1996, Congress amended the CFAA to apply to hacks involving a "protected computer"—which it defined as a computer "which is used in interstate or foreign commerce or communication." *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201(4), 110 Stat. 3488, 3493 (1996). Then, for the removal of any doubt, Congress again amended the CFAA in 2001 to expressly include computers not located in the United States. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 814(d)(1), 115 Stat. 272, 384 (2001).

This expansion of the definition of a "protected computer" was "to include qualified computers even when they are physically located outside of the United States," and thereby "preserve the ability of the United States to assist in international hacking cases." 147 Cong. Rec. S10990, S10997 (2001) (statement of Sen. Leahy). Congress recognized that deterring foreign hackers is just as important, if not more, than deterring domestic actors—after all, "[t]here are no borders or passport checkpoints in cyberspace." 142 Cong. Rec. S10886, S10889 (1996) (statement of Sen. Leahy). "[A] criminal armed with a modem and a

computer can wreak havoc on computers located in the United States from virtually anywhere in the world." *Id.*

And the United States continues to stress the importance of deterring foreign hackers today. As President Biden explained in his National Cybersecurity Strategy, "most malicious cyber activity targeting the United States is carried out by actors based in foreign countries or using foreign computing infrastructure." *National Cybersecurity Strategy*, The White House, at 30 (Mar. 1, 2023), https://tinyurl.com/y4n68wkw. "[F]oreign commercial spyware … empower[s] countries that previously lacked the ability to harm U.S. interests in cyberspace and enable[s] a growing threat from organized criminal syndicates." *Id.* at 3. It is thus fundamental to the United States's national security interest to deter the proliferation of commercial spyware by ensuring "that no [foreign] adversary," including NSO, "can evade the rule of law." *Id.* at 30. Hosting litigation in the U.S. under federal and state anti-hacking statutes allows the U.S. to hold NSO accountable for its detrimental conduct, and therefore serves important national security interests.

The district court here should have given that factor appropriate weight, and it erred in failing to do so.

B. The United States and California have fundamental interests in protecting domestic technology companies from having NSO use their products and services as spyware vectors.

The Plaintiffs in this case assert claims against NSO under federal and state statutes that specifically prohibit hacking activities and provide victims with a cause of action. *See* First Am. Compl. ¶¶ 137-58. As discussed above, the statutes creating the civil causes of action asserted here are specifically intended to deter both foreign and domestic hackers by imposing additional costs on their conduct to make them accountable to their victims. Enforcing those laws in U.S. courts as intended not only serves the national security interests discussed above, but also the substantial economic interests of the United States and California. Enforcing those laws helps protect domestic technology companies from the risk of being used as spyware vectors.

NSO traffics in spyware tools aimed at exploiting the products and services of U.S. technology companies, without the knowledge or consent of those companies. The United States and California have a powerful interest in deterring such attacks, as reflected by their

respective anti-hacking statutes. The district court improperly gave short shrift to these interests. First, the district court declined to even address the United States's interest whatsoever. Second, it failed to give any weight to California's interest. The court noted that, even "[a]ccepting [the existence of California's interest] as true for present purposes, California's interest will be amply protected" by the existence of a *different* lawsuit against NSO on similar allegations. *Dada*, 2024 WL 1024736, at *4. The district court was required to consider and afford appropriate weight to both the United States's and California's interests, and failure to do so was error.

1. The United States has an interest in protecting American companies from foreign hackers.

Across presidential administrations, the United States has repeatedly articulated strong national and economic security interests in protecting U.S. technology companies from having their products and services exploited by malicious actors. As President Obama remarked, "cyber threats [a]re one of the most serious economic national security challenges that we face as a nation." *Remarks by the President at the Cybersecurity and Consumer Protection Summit*, The White House (Feb.

13, 2015), https://tinyurl.com/y36d8vdz. "[S]o much of our computer networks and critical infrastructure are in the private sector, which means government cannot" protect against these economic and national security risks simply by safeguarding its own systems. *Id.* As explained in the National Cyber Strategy issued under President Biden, the security of American technology and networks "is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense." *National Cybersecurity Strategy*, *supra* at 23 (Introduction). Thus, the National Cyber Strategy under President Trump likewise made clear that "[p]rotecting American information networks, *whether government or private*, is vital to" "protecting the American people, the American way of life, and American interests." *National Cyber Strategy of the United States of America*, The White House, at 6 (Sept. 2018), https://tinyurl.com/2r93vwpr. These national security and economic interests are increasingly intertwined as "[t]he foundations of our economy . . . becom[e] increasingly rooted in digital

technologies. *Id.* At 14; *see also id* ("Economic security is inherently tied to our national security.").

Cyberattacks against American technology companies pose "a threat to America's economic security" because they "hurt[] American companies and cost[] American jobs." *Remarks by the President at the Cybersecurity and Consumer Protection Summit*, *supra* at 25. For example, a report by the Council of Economic Advisors estimated that "malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016" alone. *CEA Report: The Cost of Malicious Cyber Activity to the U.S. Economy*, Council of Economic Advisors (Feb. 16, 2018), https://tinyurl.com/4rx72kjn. In 2022, the average cost of a single data breach for a U.S. company reached $9.44 million. Keman Huang et al., *The Devastating Business Impacts of a Cyber Breach*, Harvard Business Review (May 4, 2023), https://tinyurl.com/ydmhpdpb. And American technology companies spend *billions* of dollars a year to protect their products and services from attack. Eric Tucker, *Tech companies pledge billions in cybersecurity investments*, AP News (Aug. 25, 2021), https://tinyurl.com/bdd2arya. When a commercial spyware provider like NSO nonetheless successfully hacks one of these

companies' products or services, that triggers a monumental, costly undertaking to contain and prevent further damage. Additionally, the harms from these attacks often cascade downstream, with each compromised device infecting other devices with which it communicates.

Given the serious national and economic security threats posed by cyberattacks against American companies such as those facilitated by NSO, it is no surprise that *amici* Microsoft and Google, as well as other technology companies, have repeatedly partnered with the federal government to enhance cybersecurity. *See, e.g.*, *FACT SHEET: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity*, The White House (Aug. 25, 2021), https://tinyurl.com/8ewdjvsf. These national security and economic concerns are also why *amici* are signatories to a set of principles that seeks to eliminate the sale and use of commercial spyware. *See, e.g., Cyber mercenaries: An old business model, a modern threat, Cybersecurity Tech Accord principles limiting offensive operations in cyberspace*, Cyber Tech Accord (Mar. 27, 2003), https://tinyurl.com/5at3a7sr.

The United States utilizes a number of deterrence mechanisms for combatting cyberattacks against American businesses, including public and private enforcement of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. *See National Cyber Strategy*, *supra* at 26, 3 ("[A]ctivity that is contrary to responsible behavior in cyberspace is deterred through the imposition of costs through cyber and non-cyber means[.]"). Congress has consistently adapted the CFAA to ensure that malicious actors are held accountable for hacking. *See e.g.*, Kerr, *supra* at 21, 1561-64. In 1986, when Congress amended the CFAA to cover private computers, it intended to penalize hackers who hijacked technology companies' systems to facilitate cybercrime. *See* 132 Cong. Rec. H3275 (1986) ("sophisticated" hackers use their technical skill to "rob banks or destroy business records or steal trade secrets," using the products of technology companies like "IBM and Apple" as "tools of the trade"). Then, in 1996, Congress expanded the CFAA's prohibition on hacking private networks from accessing information belonging to a financial institution or credit reporting agency to accessing *any* form of information. *See* Economic Espionage Act, § 201(1)(B)(ii), 110 Stat. at 3492; Kerr, *supra* at 21, 1563-64. Through these amendments,

Congress specifically intended to close the "loopholes" allowing hackers to escape responsibility for hacking American businesses. *See* 142 Cong. Rec. E1621 (1996) (statement of Rep. Goodlatte).

Congress recognized that computer hacking resulted in "staggering" costs to U.S. businesses. *Id.*; *see also id.* (the FBI and Justice Department supported the amendment because "once into a computer system, hackers have the ability to steal, modify, or destroy sensitive data"). And that includes cases in which malicious hackers exploit a company's system without stealing or destroying information. *See* 141 Cong. Rec. S9422, S9423 (1995) (statement of Rep. Kyl acknowledging that a hacker "may trespass into a computer system and view information—without stealing or destroying it"). Because the act of exploiting a system, even by itself, means "[t]he administrator of the system will spend time, money, and resources to restore security to the system. Damage occurs simply by trespassing." *Id.* Through its amendments to the CFAA, Congress resolved to "no longer accept mere trespass into computers," such as the intrusions NSO committed into Apple's servers, and to no longer "regard these intrusions as incidental." 141 Cong. Rec. at S9423; *see also* First Am. Compl. ¶¶ 2, 41. But that's

precisely what the district court did, treating as merely incidental the enormous impact NSO's operations have on American technology companies and the United States's interests in protecting them from harm.

The fact that NSO is a foreign entity does not diminish the United States's interest in protecting American technology companies from NSO's hacking activities. Most such attacks are launched by foreign actors. *See National Cybersecurity Strategy*, *supra* at 23, 30 (explaining that "most malicious cyber activity targeting the United States is carried out by actors based in foreign countries or using foreign computing infrastructure"). They are, thus, the primary parties who need to be deterred. Congress recognized that, which is why it specifically amended the CFAA to apply extraterritorially. *See United States v. Ivanov*, 175 F. Supp. 2d 367, 370 (D. Conn. 2001); s*ee also* Kerr, *supra* at 21, 1563-64 (explaining amendment history of CFAA); 142 Cong. Rec. at S10889 ("[t]here are no borders or passport checkpoints in cyberspace," and malicious hackers can "wreak havoc on computers located in the United States from virtually anywhere in the world").

That risk is exemplified by NSO. NSO traffics in the exploitation of American technology companies, and its spyware is used to surveil companies' customers. The United States has a fundamental interest, as embodied by the CFAA, to protect companies and their customers from these types of malicious attacks.

2. California also has a strong interest in protecting Californian companies from foreign hackers.

California also has a fundamental interest in protecting its technology companies from malicious actors. California has its own statutory prohibition on hacking activities—the California Comprehensive Computer Data Access and Fraud Act ("CDAFA"), California Penal Code § 502—under which the Plaintiffs bring claims against NSO. *See* First Am. Compl. ¶¶ 150-58. California's interest in protecting Californian technology companies from hackers was one of the California legislature's primary motivations in passing the CDAFA. *See* Cal. Penal Code § 502(a). Indeed, the statute itself explains: "It is the intent of the Legislature in enacting this section to expand the degree of protection afforded to individuals, businesses, and governmental agencies from tampering, interference, damage, and

unauthorized access to lawfully created computer data and computer systems." *Id.* As the statute recognizes, "the proliferation of computer technology has resulted in a concomitant proliferation of computer crime and other forms of unauthorized access to computers, computer systems, and computer data." *Id.* The "protection of the integrity of all types and forms of lawfully created computers, computer systems, and computer data is vital to the protection of the privacy of individuals as well as to … business concerns." *Id.*

Those business concerns are especially important to California—the state with more technology companies than any other state in the union. California.gov, *High Tech*, https://tinyurl.com/3ektsjkb. "California's tech industry delivers an economic impact of $536 billion, or 16.7% of the state economy." CompTIA, *California tech workforce grows in depth and breadth: CompTIA releases year in review State of the Tech Workforce report* (Mar. 30, 2023), https://tinyurl.com/2ap8pu8v. An estimated 55,868 technology businesses call California home. *Id.* California is thus "a national leader in the area of information systems," which is why, in passing the CDAFA, it sought to "make an all-out

effort to protect this important industry." Background Sheet for the Senate Judiciary Committee on Senate Bill 255 (Davis) at 1.

The district court failed to afford appropriate weight to California's interest in protecting U.S. technology companies based in California from having their products and services exploited by NSO and its clients. The court improperly brushed off that substantial state interest, concluding that even if there were such an interest, it would be adequately redressed by Apple's separate lawsuit against NSO. *See Dada*, 2024 WL 1024736 at *4 ("[E]ven accepting [California's interest] 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."). But whether California is separately interested in a different lawsuit has no bearing on whether California (or the United States, for that matter) has an interest in the present lawsuit. The forum's interest in the subject matter of litigation does not diminish with each case that speaks to that interest.

Every case presents its own issues and challenges, including those arising from the parties involved, their counsel, their resources, and business or reputational considerations outside of the litigation. So, the

notion that a substantial state interest may hinge entirely on the success of any one particular case is speculative and contrary to common sense. Moreover, the deterrent effect of imposing litigation costs on bad actors is *enhanced*, not diminished, by each and every action holding bad actors accountable. Congress and the California legislature have specifically provided causes of action to bring companies like NSO to account for their hacking conduct. For NSO to be properly deterred from engaging in this conduct in the future, U.S. courts should not be so quick to shut the courthouse doors.

Accordingly, the district court erred in negating California's fundamental interest in this lawsuit.

CONCLUSION

For the foregoing reasons, this Court should reverse and remand the district court's order.

Respectfully submitted,

/s/David A. Simon
David A. Simon
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
1440 New York Avenue, N.W.
Washington, D.C. 20005
(202) 371-7120

William E. Ridgway
SKADDEN, ARPS, SLATE, MEAGHER & FLOM LLP
320 S. Canal St.
Chicago, Illinois 60606
(312) 407-0449

Counsel for Amicus Curiae Google LLC

/s/Robert M. Loeb
Robert M. Loeb
ORRICK, HERRINGTON & SUTCLIFFE LLP
2100 Pennsylvania Avenue, NW
Washington, DC 20037
(202) 339-8400

Rachael Jensen
ORRICK, HERRINGTON & SUTCLIFFE LLP
300 West 6th Street, Suite 1850
Austin, TX 78701

Counsel for Amicus Curiae Microsoft Corporation, GitHub, Inc., LinkedIn Corporation, Trend Micro, Inc., and Big Cloud Consultants, LLC

July 22, 2024

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 24-2179

I am the attorney or self-represented party.

This brief contains ____6,295_____ words, including _____0_____ words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[ ] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[X] is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
- [ ] it is a joint brief submitted by separately represented parties.
- [ ] a party or parties are filing a single brief in response to multiple briefs.
- [ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Robert M. Loeb **Date** July 22, 2024
*(use "*s/[typed name]*" to sign electronically-filed documents)*