No. 20-16408

IN THE

United States Court of Appeals for the Ninth Circuit

NSO GROUP TECHNOLOGIES LTD. ET AL.,

Defendants-Appellants,

v.

WHATSAPP INC. ET AL.,

Plaintiffs-Appellees.

On Appeal from the United States District Court for the Northern District of California
No. 4:19-cv-07123-PJH

BRIEF FOR AMICI CURIAE MICROSOFT CORP., CISCO SYSTEMS, INC., GITHUB, INC., GOOGLE LLC, LINKEDIN CORPORATION, VMWARE, INC., AND INTERNET ASSOCIATION IN SUPPORT OF PLAINTIFFS-APPELLEES

Michael Trinh
GOOGLE LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043
(650) 253-0000

Counsel for Amicus Curiae Google LLC

Mark Parris
Carolyn Frantz
Paul Rugani
Alyssa Barnard-Yanni
ORRICK, HERRINGTON & SUTCLIFFE LLP
701 5th Ave., Ste. 5600
Seattle, WA 98104
(206) 839-4300

Counsel for Amici Curiae Microsoft Corp., Cisco Systems, Inc., GitHub, Inc., LinkedIn Corporation, VMware, Inc., and Internet Association

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 Cisco Systems, Inc. ("Cisco") is a publicly held corporation. Cisco does not have a parent corporation and no publicly held corporation holds 10% or more of its 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 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 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 VMware, Inc. ("VMware") is majority-owned by a series of entities including VMW Holdco LLC, EMC Corporation, Dell Inc., Denali Intermediate Inc., and Dell Technologies Inc. The lone publicly held corporation directly or indirectly owning 10% or more of VMware is Dell Technologies Inc.

Amicus Internet Association ("IA") is not a publicly held corporation. It does not have a parent corporation and no publicly held corporation holds 10% or more of its stock.

GOOGLE LLC

/s/Michael Trinh
Michael Trinh
Counsel for Amicus Google LLC

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/Mark Parris
Mark Parris
Counsel for Amici Curiae Microsoft Corp., Cisco Systems, Inc., GitHub, Inc., LinkedIn Corporation, VMware, Inc., and Internet Association

TABLE OF CONTENTS

Page

CORPORATE DISCLOSURE STATEMENT i
TABLE OF AUTHORITIES iv
INTERESTS OF *AMICI CURIAE* 1
INTRODUCTION AND SUMMARY OF ARGUMENT 5
STATEMENT OF THE CASE 10
ARGUMENT 12
Allowing Companies Like NSO To Deploy Powerful Cyber-Surveillance Tools Across U.S. Systems Creates Large-Scale, Systemic Cybersecurity Risk 12
A. Expanding immunity to private cyber-surveillance companies would greatly increase access to and use of cyber-surveillance tools. 13
1. Expanding immunity would increase the number of governments and companies with access to these tools. 13
2. Expanding immunity would also increase the use of dangerous cyber-surveillance tools. 17
B. Increased access to and use of cyber-surveillance tools significantly raises systemic cybersecurity risk. 21
C. These increased systemic risks would do extensive damage. 24
CONCLUSION 28
CERTIFICATE OF COMPLIANCE

TABLE OF AUTHORITIES

Page(s)

Statutes

Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ..... 1, 11

Federal Rule of Appellate Procedure 29(a)(4)(e) 1

Other Authorities

About Software Management and Patch Releases, Oracle Corporation, https://tinyurl.com/y5nvr7j8 18

Amnesty International Among Targets of NSO-powered Campaign, Amnesty International (Aug. 1, 2018), https://tinyurl.com/y5vg6chz 12

Andy Greenberg, *Hacking Team Breach Shows a Global Spying Firm Run Amok*, Wired (July 6, 2015), https://tinyurl.com/y2u5shjj 16, 22

Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, Wired (Apr. 17, 2015), https://tinyurl.com/yyyk6n5w 20

Andy Greenberg, *Strange Journey of an NSA Zero-Day—Into Multiple Enemies' Hands*, Wired (May 7, 2019), https://tinyurl.com/y2nrvkf2 ..... 7, 8, 26

Andy Greenberg, *This Map Shows the Global Spread of Zero-Day Hacking Techniques*, Wired (April 6, 2020), https://tinyurl.com/tc8kwg9 16

Andy Greenberg, *Triple Meltdown: How So Many Researchers Found a 20-Year-Old Chip Flaw at the Same Time*, Wired (Jan. 7, 2018), https://tinyurl.com/ydbdjfp7 25

Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired (Aug. 22, 2018), https://tinyurl.com/y3o3pxq8 ..... 6, 7, 26, 28

Azam Ahmed, *A Journalist Was Killed in Mexico. Then His Colleagues Were Hacked.*, N.Y. Times (Nov. 27, 2018), https://tinyurl.com/y6zu8pth 12

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* 5 (Aug. 24, 2016), https://tinyurl.com/y3uvmlev 22

Bill Marczak et al., *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*, The Citizen Lab (Oct. 1, 2018), https://tinyurl.com/y9yyhaz3 12

Christopher Bing & Joel Schectman, *Inside the UAE's Secret Hacking Team of American Mercenaries: Ex-NSA operatives reveal how they helped spy on targets for the Arab monarchy—dissidents, rival leaders and journalists*, Reuters (Jan. 30, 2019), https://tinyurl.com/y9qnsbs4 21

Communications Security Establishment, *CSE's Equities Management Framework* (Mar. 11, 2019), https://tinyurl.com/y3mj3p97 19

David Murphy, *This New Android Malware Can Survive a Factory Reset*, LifeHacker (Oct. 30, 2019), https://tinyurl.com/yxwjut25 27

David Voreacos et al., *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, Bloomberg (Dec. 2, 2019), https://tinyurl.com/usklyf3 6

How Google handles security vulnerabilities, Google LLC, https://tinyurl.com/lxspq7v 17

How to detect spyware to safeguard your privacy?, Kaspersky Lab, https://tinyurl.com/y679odja 27

Ian Levy, National Cyber Security Centre, *Equities process: Publication of the UK's process for how we handle vulnerabilities* (Nov. 29, 2018), https://tinyurl.com/y4x5eeft 19

John Scott-Railton et al., *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*, The Citizen Lab (Feb. 11, 2017), https://tinyurl.com/ya3tgrhr 12

Kathleen Metrick et al., *Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill*, FireEye (Apr. 6, 2020), https://tinyurl.com/qrxk2vk) 16

Keith Breene, *Who are the cyberwar superpowers?*, World Economic Forum (May 4, 2016), https://tinyurl.com/y359xprj 15

Kelly Jackson Higgins, *Unpatched Vulnerabilities the Source of Most Data Breaches*, Dark Reading (April 5, 2018), https://tinyurl.com/y4xat346 26

Lance Whitney, *How to handle the public disclosure of bugs and security vulnerabilities*, TechRepublic (Sept. 19, 2019), https://tinyurl.com/y3vupgfx 18

Lillian Ablon & Andy Bogart, RAND Corporation, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* (2017), https://tinyurl.com/y27ssfau 7, 25

Lorenzo Franceschi-Bicchierai, *The Vigilante Who Hacked Hacking Team Explains How He Did It*, Vice (Apr. 15, 2016) https://tinyurl.com/y284rpou 22

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/y39pzhtc13, 14, 15, 21

Mehul Srivastava & Tom Wilson, *Inside the WhatsApp hack: how an Israeli technology was used to spy*, Financial Times (Oct. 29, 2019), https://tinyurl.com/y8zwkcl9 11

Microsoft's Approach to Coordinated Vulnerability Disclosure, Microsoft Corporation, https://tinyurl.com/y8snnzda 17

Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times (July 13, 2013), https://tinyurl.com/yypwwa8c 20

Nicole Perlroth et al., *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. Times (June 27, 2017), https://tinyurl.com/ydco89o5 6

Nicole Perlroth et al., *How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks*, N.Y. Times (May 6, 2019), https://tinyurl.com/yysm2c6a 8, 23

Patrick Howell O'Neill, *The Lucrative Government Spyware Industry Has a New 'One-Stop-Shop' for Hacking Everything*, Gizmodo (Feb. 15, 2019), https://tinyurl.com/yxwwuktz 14

Priscilla Moriuchi & Bill Ladd, *China's Ministry of State Security Likely Influences National Network Vulnerability Publications* (2017), https://tinyurl.com/y32rn83m 19

Scott Shane et al., *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, N.Y. Times (Nov. 12, 2017), https://tinyurl.com/yc7zvxap 7

Scott Steadman, *The Covert Reach of NSO Group*, Forensic News (Apr. 29, 2020), https://tinyurl.com/y4vsrbh2 21

Statement from the Press Secretary, The White House (Feb. 15, 2018), https://tinyurl.com/y3fw6yea 6

Trey Herr et al., *Taking Stock: Estimating Vulnerability Rediscovery* (July 2017), https://tinyurl.com/y2udejph 7

U.S. Department of State, *State Sponsors of Terrorism*, https://tinyurl.com/y3vtudya 22

Vindu Goel & Nicole Perlroth, *Spyware Maker NSO Promises Reform but Keeps Snooping*, N.Y. Times (Nov. 10, 2019), https://tinyurl.com/yxd2sne5 11

VMware, Advisory VMSA-2020-0027.2 (Nov. 23, 2020), https://tinyurl.com/y2ofvx4c 19

Vulnerabilities Equities Policy and Process for the United States Government (Nov. 15, 2017), https://tinyurl.com/ycj6dzw3 19

What is Ransomware?, Kaspersky Lab, https://tinyurl.com/y6w5ecl6 5

What is Spyware?, Kaspersky Lab, https://tinyurl.com/y4h43vsy 10

INTERESTS OF *AMICI CURIAE*[1]

Private-sector companies like NSO Group Technologies Ltd. ("NSO") are investing heavily in creating cyber-surveillance tools and selling "cyber-surveillance as a service" to foreign governments and other customers. These tools allow the user to 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. Foreign governments are then using those surveillance tools, bought on the open market, to spy on human rights activists, journalists, and others, including U.S. citizens. The Computer Fraud and Abuse Act and other U.S. laws make it illegal to access a computing device without proper authorization. *See*, *e.g.*, 18 U.S.C. § 1030. Here, NSO seeks immunity from these laws through an expansion of the common law of foreign sovereign immunity to cover private companies' actions on behalf of foreign-government customers.

---

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(e), *amici* certify that no counsel for a party authored the brief in whole or in part, and no person or entity other than *amici* 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.

The cyber-surveillance tools at issue here take significant time, investment, and research to develop, as they need to evade detection by the device being attacked (e.g., a phone or personal computer), as well as each and every application from which the tools wish to extract information. Collectively, *amici* offer products and services, and rely on systems, that may be targeted by malicious actors, both foreign and domestic. *Amici* accordingly work hard to design and develop secure products, services, and systems, and to protect them—and, more importantly, the people who use them—from intrusion. Their efforts make up part of the more than $120 billion spent on cybersecurity worldwide every year. These investments preserve the functionality of their products and services, but also serve to maintain customer trust and privacy.

- Microsoft Corporation ("Microsoft") is a leading innovator in computer software and online services. Its mission: To help individuals and businesses throughout the world realize their full potential by transforming the way people work, play, and communicate. Microsoft develops, manufactures, licenses, and supports a wide range of programs in service of that mission, including the flagship Windows operating system, the Microsoft Office suite, the Surface tablet, and the Xbox gaming system. Microsoft also acts as a global cybersecurity advocate across the industry to ensure safer and more trusted computer experiences for everyone.

- Cisco Systems, Inc. ("Cisco") is a worldwide leader in developing, implementing, and providing the technologies behind networking, communications, security, and information technology products and services. It develops and provides a broad range of networking products and services that enable seamless communication among individuals, businesses, public institutions, government agencies, and service providers. Cisco takes a security-first approach and has created a portfolio designed to prevent, detect, and remediate a cyber-attack and to integrate security across networking domains.

- GitHub, Inc. ("GitHub") is the largest software code hosting and software development platform in the world. GitHub is committed to building the global platform for developer collaboration—one that everyone can use to secure the world's software, together. GitHub helps developers stay ahead of security issues, leverage the community's security expertise, and use open source securely. GitHub stands against hoarding and selling exploits and attack or surveillance tools. Such tools could be used not only to infiltrate GitHub, but the millions of developers and open source projects which rely on its platform, and the software supply chain which depends on them.

- Google LLC ("Google") is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of online services, products, and platforms—including Search, Gmail, Maps, YouTube, Android, and Chrome, as well as enterprise-focused services such as Google Cloud Platform and G Suite—that are used by people and businesses throughout the United States and around the world.

- LinkedIn Corporation ("LinkedIn") hosts a widely used social network, with over 720 million members worldwide and over 170 million members in the United States. LinkedIn's

mission is to connect the world's professionals to enable them to be more productive and successful.

- VMware, Inc. ("VMware") provides cloud computing and virtualization software and services and technologies to enable the development of applications in modern environments, as well as products and services designed to secure those environments.

- Internet Association ("IA") represents the interests of leading internet companies and their customers, and it is the only trade association that exclusively represents such companies on matters of public policy. IA's mission is to foster innovation, promote economic growth, and empower people through the free and open internet. A list of IA's members is available at https://internetassociation.org/our-members/.

Amici have an interest in ensuring that entities who access their products, services, and systems in violation of U.S. law are held accountable in U.S. courts. More broadly, *amici* have an interest in decreasing systemic cybersecurity risk by helping to ensure that cyberspace is itself secure. In this brief, *amici* explain how immunizing uses of privately developed cyber-surveillance tools would dramatically increase systemic cybersecurity risk.

INTRODUCTION AND SUMMARY OF ARGUMENT

On June 27, 2017, the second-largest bank in Ukraine fell victim to a ransomware attack[2] that crippled 90 percent of the bank's computers. The attack spread quickly throughout the country. At the nuclear power plant in Chernobyl—the site of the largest nuclear disaster in history—the computers that monitor radiation levels went down, forcing workers to conduct monitoring manually. ATMs stopped working. The post office was forced to shut down, followed by hospitals, power companies, and airports. According to the Ukrainian minister of infrastructure, as a result of the attack, "The government was dead."

But the attack did not stop at the Ukrainian border. Denmark-based Maersk, the largest shipping company in the world, lost use of its computers, servers, routers, and even desk phones for days, resulting in stranded container ships and closed ports across the globe. A Cadbury chocolate factory in Australia had to stop production. In the U.S., Pennsylvania hospitals had to cancel surgeries. Pharmaceutical giant

[2] "Ransomware is a malicious software that infects [a] computer and displays messages demanding a fee to be paid in order for [a] system to work again." *What is Ransomware?,* Kaspersky Lab, https://tinyurl.com/y6w5ecl6.

Merck, which lost 30,000 computers and 7,500 servers to the attack, had to stop production of the Gardasil 9 vaccine for two weeks, and researchers reported losing years of research. All told, the attack—which came to be known as "NotPetya"—affected more than 60 countries and inflicted more than $10 billion in damage.[3] According to the United States government, it was "the most destructive and costly cyber-attack in history." Statement from the Press Secretary, The White House (Feb. 15, 2018), https://tinyurl.com/y3fw6yea.

Mounting an attack like NotPetya is a complex, expensive, and time-consuming undertaking. As noted above, *see supra* at 2, companies like Microsoft and other *amici* devote substantial time and resources to protecting their products, services, and systems from intrusion. Accordingly, someone who wishes to launch a cyberattack must figure out a way to access a device undetected—often by making use of what is

[3] The above narrative of NotPetya was sourced from the following articles: Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, Wired (Aug. 22, 2018), https://tinyurl.com/y3o3pxq8 (hereinafter "*Untold Story*"); Nicole Perlroth et al., *Cyberattack Hits Ukraine Then Spreads Internationally*, N.Y. Times (June 27, 2017), https://tinyurl.com/ydco89o5; David Voreacos et al., *Merck Cyberattack's $1.3 Billion Question: Was It an Act of War?*, Bloomberg (Dec. 2, 2019), https://tinyurl.com/usklyf3.

known in cybersecurity parlance as a "zero-day vulnerability."[4] By way of example, the NotPetya attack (eventually attributed to Russia) relied on a cyber-tool called "EternalBlue," which made use of a vulnerability in the Windows operating system. *See Untold Story*, *supra* note 3. But Russia did not itself develop the technology employed in the attack. Russia seemingly obtained EternalBlue from an online leak by a "mysterious hacker group known as the Shadow Brokers"—but it has been widely accepted that the tool was actually created by the U.S. National Security Agency (NSA). Andy Greenberg, *Strange Journey of an NSA Zero-Day—Into Multiple Enemies' Hands*, Wired (May 7, 2019), https://tinyurl.com/y2nrvkf2 (hereinafter "*Strange Journey*"); *see also* Scott Shane et al., *Security Breach and Spilled Secrets Have Shaken the N.S.A. to Its Core*, N.Y. Times (Nov. 12, 2017),

[4] "[V]ulnerabilities are flaws or features in code that allow a third party to manipulate the [device] running [the code]." Trey Herr et al., *Taking Stock: Estimating Vulnerability Rediscovery* 3 (July 2017), https://tinyurl.com/y2udejph. "The term *zero-day* refers to the number of days a … vendor has known about the vulnerability." Lillian Ablon & Andy Bogart, RAND Corporation, *Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and Their Exploits* ix (2017), https://tinyurl.com/y27ssfau. Thus, a "zero-day vulnerability" is a "flaw in code that [the vendor] doesn't know about." Andy Greenberg, *The Strange Journey of an NSA Zero-Day—Into Multiple Enemies' Hands*, Wired (May 7, 2019), https://tinyurl.com/y2nrvkf2.

https://tinyurl.com/yc7zvxap. And the Shadow Brokers were not the only ones to steal this tool from the NSA; press reports indicate that China did as well, apparently by reverse-engineering it after they detected it deployed against them. *See Strange Journey*, *supra* at 7; *see also* Nicole Perlroth et al., *How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them for Attacks*, N.Y. Times (May 6, 2019), https://tinyurl.com/yysm2c6a (hereinafter "*Chinese Spies*").

No matter how damaging, the actions of the NSA in creating EternalBlue and Russia in using it would be protected from liability by long-standing principles of sovereign immunity. The risks posed by governments creating and using these tools *themselves*, however, are minimized considerably by the fact that only a handful of countries have the ability to independently create or use such tools. Moreover, the countries with such capabilities have internal processes to determine when it is worth the risk to the broader cybersecurity ecosystem (which they and their citizens also depend on) to do so.

But thanks to a nascent—and profitable—private industry that has sprung up to develop and then use powerful cyber-tools for foreign-government customers, these tools are much more widely available than

they used to be. Accordingly, this Court must now decide whether to radically expand the risks these powerful tools pose by also immunizing *private* companies' use of commercially developed cyber-surveillance tools when they act on behalf of their foreign-government customers. The NotPetya attack shows just how dangerous cyber-surveillance tools can be—in particular, how they can be repurposed to cause harms far beyond their intended uses (even if those uses are themselves appropriate). If the NSA—which has a technical capability advanced enough to create its own powerful cyber-surveillance tools and an equally advanced policy infrastructure designed to restrict the use of such tools only to appropriate cases—could not keep EternalBlue under control, what chance is there to keep these powerful tools from spiraling out of control if they are made and used indiscriminately by private companies on behalf of any government who is willing to pay for them?

Expanding foreign sovereign immunity to private companies that use their own cyber-surveillance tools at the behest of their numerous foreign-government customers would dramatically increase the creation and use of cyber-surveillance tools globally. In particular, it would place these tools in the hands of more governments, including governments

likely to engage in riskier behaviors and at greater risk of losing control of such tools. As more companies develop these tools and more governments buy them, the risk that they will fall into the wrong hands increases exponentially and threatens all of us. This court should decline to extend foreign sovereign immunity to the use of cyber-surveillance tools by private companies at the behest of foreign government customers.

STATEMENT OF THE CASE

Defendants NSO and Q Cyber Technologies Ltd. (collectively, NSO) are Israeli corporations that develop, sell, and operate "surveillance technology or 'spyware' designed to intercept and extract information and communications from mobile phones and devices" for their foreign-government clients. ER 53, 66.[5] One of NSO's products is "Pegasus," a program "designed to be remotely installed and enable the remote access and control of information—including calls, messages, and location—on mobile devices." ER 66. Until recently, Pegasus could

[5] "Spyware is loosely defined as malicious software designed to enter your … device, gather data about you, and forward it to a third-party without your consent." *What is Spyware?,* Kaspersky Lab, https://tinyurl.com/y4h43vsy.

be remotely installed through the WhatsApp app on a person's mobile device: the program used vulnerabilities in WhatsApp's code to "emulate legitimate … network traffic," thereby "transmit[ting] malicious code—undetected." ER 69. As a result, Pegasus could be installed on a device simply by calling that device—"even when the [user] did not answer the call." *Id.*

Pegasus was installed in this manner on at least 1,400 mobile devices. ER 70.[6] WhatsApp and Facebook (which handles cybersecurity for WhatsApp) eventually identified and closed the vulnerabilities NSO had used. ER 63, 71. WhatsApp and Facebook then sued NSO in federal court, alleging NSO had gained unauthorized access to WhatsApp's network and servers in violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, and also state law. ER 71-74. NSO moved to dismiss, arguing it should be afforded foreign sovereign immunity because it accessed WhatsApp as an agent of its foreign-government customers.

---

[6] For information about some of the targets, see, *e.g.*, Vindu Goel & Nicole Perlroth, *Spyware Maker NSO Promises Reform but Keeps Snooping*, N.Y. Times (Nov. 10, 2019), https://tinyurl.com/yxd2sne5 (lawyers and human rights activists in India); Mehul Srivastava & Tom Wilson, *Inside the WhatsApp hack: how an Israeli technology was used to spy*, Financial Times (Oct. 29, 2019), https://tinyurl.com/y8zwkcl9 (political dissidents from Rwanda).

The district court denied NSO's motion in relevant part, holding that, as a private company, NSO was not entitled to sovereign immunity. ER 9-15. NSO now appeals.

ARGUMENT

Allowing Companies Like NSO To Deploy Powerful Cyber-Surveillance Tools Across U.S. Systems Creates Large-Scale, Systemic Cybersecurity Risk.

Cyber-surveillance tools like NSO's Pegasus are powerful, and dangerous. Such tools depend on vulnerabilities in code that allow one person to access another person's device, network, or system. If those tools are misused, the results can be disastrous. Foreign governments may use the technology in problematic ways,[7] but beyond idiosyncratic

[7] NSO attempts to characterize its customers' intended uses as appropriate. There is substantial reason to doubt this characterization. According to public reporting, foreign governments have used NSO's tools to surveil a wide variety of private citizens, from journalists to human rights activists to supporters of a soda tax. *See*, *e.g.*, Azam Ahmed, *A Journalist Was Killed in Mexico. Then His Colleagues Were Hacked.*, N.Y. Times (Nov. 27, 2018), https://tinyurl.com/y6zu8pth; *Amnesty International Among Targets of NSO-powered Campaign*, Amnesty International (Aug. 1, 2018), https://tinyurl.com/y5vg6chz; Bill Marczak et al., *The Kingdom Came to Canada: How Saudi-Linked Digital Espionage Reached Canadian Soil*, The Citizen Lab (Oct. 1, 2018), https://tinyurl.com/y9yyhaz3; John Scott-Railton et al., *Bitter Sweet: Supporters of Mexico's Soda Tax Targeted With NSO Exploit Links*, The Citizen Lab (Feb. 11, 2017), https://tinyurl.com/ya3tgrhr.

misuse is a much greater systemic risk. Widespread creation and deployment of these tools by private companies acting for profit dramatically increases the risk that these vulnerabilities will be obtained and exploited by malicious actors *other* than the initial customer to cripple infrastructure, commit large-scale financial crime, or cause other catastrophic damage.

A. Expanding immunity to private cyber-surveillance companies would greatly increase access to and use of cyber-surveillance tools.

A robust, unchecked, commercial market for cyber-surveillance tools would dramatically increase the number of governments and private companies with access to them. Given the nature of private industry, it would also significantly increase the frequency with which they would be used.

1. Expanding immunity would increase the number of governments and companies with access to these tools.

Recent years have seen a "proliferation of companies trying to replicate NSO's success and compete in an estimated $12 billion market for so-called lawful intercept spyware." 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. Just last year, for example, some of the newcomers in this "rising industry" announced the creation of the "Intelligence Alliance," or "Intellexa," to compete with NSO. Patrick Howell O'Neill, *The Lucrative Government Spyware Industry Has a New 'One-Stop-Shop' for Hacking Everything*, Gizmodo (Feb. 15, 2019), https://tinyurl.com/yxwwuktz. The industry has drawn considerable private equity investment, another signal of the perceived vitality of this business. *See id.*; Mazzetti et al., *supra* at 13.[8]

Expanding immunity would hamper efforts to stop this worrying expansion, and, indeed, encourage even more companies, with even more clients, to create and use these tools. After all, the risk of liability in U.S. courts operates as a deterrent to business models that depend on violating U.S. law—particularly for nascent companies in an up-and-coming industry, which cannot as easily absorb the monetary cost of such liability. Expanding immunity, however, would remove that

[8] Indeed, private equity firm Francisco Partners owned a controlling stake in NSO until recently, when its founders succeeded in raising sufficient capital to buy back majority control. *See* Mazzetti et al., *supra* at 13.

deterrent, and encourage companies to capitalize on this emerging market.

The consequence of an immunized and expanding private cyber-surveillance industry: more foreign governments with powerful and dangerous cyber-surveillance tools. After all, tools like Pegasus are expensive and time-consuming to develop; they also require a high level of technical skill. Accordingly, only a limited number of countries are currently capable of developing these types of tools themselves. *See, e.g.*, Keith Breene, *Who are the cyberwar superpowers?*, World Economic Forum (May 4, 2016), https://tinyurl.com/y359xprj (listing the United States, China, Russia, Israel, the United Kingdom, Iran, and North Korea as key players in this space). But cyber-surveillance companies lower the barriers to entry, making such tools available to far more countries: Instead of spending billions to fund an agency like the NSA, foreign governments can buy Pegasus from NSO for a few million. *See* Mazzetti et al., *supra* at 13. And unsurprisingly, if governments can purchase such tools easily on the open market from private companies, more governments will make use of them.

Indeed, the beginnings of this phenomenon are already apparent. Between 2012 and 2015, a report identifying government-sponsored cyberattacks attributed all of them to just five countries: Russia, China, North Korea, France, and Israel. See Andy Greenberg, *This Map Shows the Global Spread of Zero-Day Hacking Techniques*, Wired (April 6, 2020), https://tinyurl.com/tc8kwg9 (discussing Kathleen Metrick et al., *Zero-Day Exploitation Increasingly Demonstrates Access to Money, Rather than Skill*, FireEye (Apr. 6, 2020), https://tinyurl.com/qrxk2vk). Between 2016 and 2018, however, the cast of characters changed: among others, the United Arab Emirates and Uzbekistan joined the ranks of confirmed attackers. *Id.* And that likely represents a small subset of the countries now mounting such attacks; countries that have been identified in public reporting as clients of cyber-surveillance companies like NSO include Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakhstan, Mexico, Morocco, Nigeria, Oman, Saudi Arabia, and Sudan. *See*, *e.g.*, Andy Greenberg, *Hacking Team Breach Shows a Global Spying Firm Run Amok*, Wired (July 6, 2015), https://tinyurl.com/y2u5shjj (hereinafter "*Spying Run Amok*").

2. Expanding immunity would also increase the use of dangerous cyber-surveillance tools.

Even beyond the simple (and significant) fact that more governments and companies will have access to these tools, the very nature of the commercial market will result in their increased use. Private companies and governments have very different interests when considering whether to deploy a found vulnerability or to disclose it to the vendor so that it can be fixed.

Governments that have the technical sophistication to find so-called "zero-day vulnerabilities," *see supra* at 7 note 4, frequently disclose them to the vendor, rather than using them. This type of disclosure, called "responsible disclosure," or "Coordinated Vulnerability Disclosure," "allows the vendor the opportunity to diagnose and offer fully tested updates, workarounds, or other corrective measures before any party discloses detailed vulnerability or exploit information to the public." *Microsoft's Approach to Coordinated Vulnerability Disclosure*, Microsoft Corporation, https://tinyurl.com/y8snnzda; *see also How Google handles security vulnerabilities*, Google LLC, https://tinyurl.com/lxspq7v. Such an update is commonly known as a

"patch." *See About Software Management and Patch Releases*, Oracle Corporation, https://tinyurl.com/y5nvr7j8.[9]

In deciding whether to disclose an identified vulnerability, governments make use of established deliberative processes. While governments have an interest in using cyber-surveillance tools for their own purposes, they also take into consideration the importance of minimizing systemic cybersecurity risks.

For example, the United States has an interagency "Vulnerabilities Equities Process" (VEP), comprised of representatives from no fewer than eight executive departments, designed to:

> prioritize the public's interest in cybersecurity and to protect core Internet infrastructure, information systems, critical infrastructure systems, and the U.S. economy through the disclosure of vulnerabilities … absent a demonstrable, overriding interest in the use of the vulnerability for lawful intelligence, law enforcement, or national security purposes.

---

[9] In certain circumstances, a finder may choose to publicly report the existence of a vulnerability rather than privately disclosing it to the vendor. See Lance Whitney, *How to handle the public disclosure of bugs and security vulnerabilities*, TechRepublic (Sept. 19, 2019), https://tinyurl.com/y3vupgfx. This is fairly rare, and is almost always in service of trying to pressure a vendor to move faster to issue patches. *Id.*

Vulnerabilities Equities Policy and Process for the United States Government 1 (Nov. 15, 2017), https://tinyurl.com/ycj6dzw3. According to the United States, "[i]n the vast majority of cases, responsibly disclosing a newly discovered vulnerability is clearly in the national interest." *Id.* For example, just recently, the NSA disclosed to VMware a vulnerability in its software, and VMware was able to release a patch. *See* VMware, Advisory VMSA-2020-0027.2 (Nov. 23, 2020), https://tinyurl.com/y2ofvx4c.

Other countries have similar vulnerabilities evaluation programs, including, it appears, China. *See, e.g.*, Ian Levy, National Cyber Security Centre, *Equities process: Publication of the UK's process for how we handle vulnerabilities* (Nov. 29, 2018), https://tinyurl.com/y4x5eeft (describing the United Kingdom's evaluation process, in which the "default position is to disclose the problem"); Communications Security Establishment, *CSE's Equities Management Framework* (Mar. 11, 2019), https://tinyurl.com/y3mj3p97 (detailing Canada's equities process); Priscilla Moriuchi & Bill Ladd, *China's Ministry of State Security Likely Influences National Network Vulnerability Publications* 3, 15 (2017), https://tinyurl.com/y32rn83m

(finding "evidence of a formal vulnerability evaluation process" in China). This is unsurprising; the same countries that have the means to develop cyber-surveillance tools also have a reason to be careful about the risks the use of those tools may introduce into the ecosystem—their industries and citizens are likely to be seriously affected by cyberattacks, and their opponents are likely to target them or their allies with the same tools if those tools become compromised.

Private cyber-surveillance companies like NSO, by contrast, do not operate with the same caution. When such actors locate a zero-day vulnerability, they do not disclose it to the vendor; instead, their business model is to exploit the vulnerability for profit, either by using it directly or selling it to someone who will.[10] And it is a profitable business indeed. According to reports, for example, a single "zero-day exploit in Apple's iOS operating system sold for $500,000." Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. Times (July 13, 2013), https://tinyurl.com/yypwwa8c. Ready-made products that exploit such

[10] See, e.g., *See* Andy Greenberg, *New Dark-Web Market Is Selling Zero-Day Exploits to Hackers*, Wired (Apr. 17, 2015), https://tinyurl.com/yyyk6n5w.

vulnerabilities are even more valuable. After NSO developed Pegasus, for example, its first Pegasus client (Mexico) reportedly paid $15 million for NSO's hardware and software—and an additional $77 million for NSO's surveillance-management services. Mazzetti et al., *supra* at 13. In 2019, NSO was valued at just under $1 billion. *See id.*[11]

B. Increased access to and use of cyber-surveillance tools significantly raises systemic cybersecurity risk.

This growing commercial market for cyber-surveillance-as-a-service raises systemic cybersecurity risk in several ways.

First, the developers of these powerful tools, and their foreign government clients, can fall victim to hacks and leaks. This is a troublingly common phenomenon. In the private sector, the Italian company Hacking Team—one of NSO's competitors—was itself hacked

[11] To protect these profits, companies like NSO operate through what has been described as "a dizzying web of shell companies." Scott Steadman, *The Covert Reach of NSO Group*, Forensic News (Apr. 29, 2020), https://tinyurl.com/y4vsrbh2. They also invest heavily in recruiting former members of the intelligence community, leveraging their experience to help build technologies that are able to evade detection. *See, e.g.*, Christopher Bing & Joel Schectman, *Inside the UAE's Secret Hacking Team of American Mercenaries: Ex-NSA operatives reveal how they helped spy on targets for the Arab monarchy—dissidents, rival leaders and journalists*, Reuters (Jan. 30, 2019), https://tinyurl.com/y9qnsbs4.

in 2015. *See Spying Run Amok*, *supra* at 16. Not only did the hacker expose some of Hacking Team's clients (including Sudan—a country that has been designated by the United States as a state sponsor of terrorism since 1993, *see* U.S. Department of State, *State Sponsors of Terrorism*, https://tinyurl.com/y3vtudya), 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.

The more robust the private cyber-surveillance-as-a-service market is, the greater this risk. The larger the number of companies offering this service and the more clients they have, the more places there are for malicious actors to find these tools—and the more likely it is that these tools will be stored in an insecure manner, making it easier for them to be stolen.

Second, the targets of these tools can observe, reverse-engineer, and then use these tools for their own purposes. In 2016, for example, a human rights activist in the United Arab Emirates, Ahmed Mansoor, was the target of an attack that appeared to use NSO's Pegasus spyware. *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 5, 9-11 (Aug. 24, 2016), https://tinyurl.com/y3uvmlev. Mansoor was suspicious of messages he received on his phone, so he sent them to researchers at The Citizen Lab, a cybersecurity laboratory based out of the University of Toronto. The researchers were able to identify "a chain of zero-days exploits … that would have remotely jailbroken Mansoor's stock iPhone6." *Id*. at 5. Thankfully, Mansoor and the Citizen Lab researchers reported the zero-day vulnerabilities they identified to Apple, which developed a patch. *Id*. at 6. But not all targets of cyber-surveillance can be expected to do the same. In 2016, for example, Chinese intelligence agents "captured [the NSA's hacking tools] from an [NSA] attack on [Chinese] computers," and then "repurposed them … to attack American allies and private companies in Europe and Asia." *Chinese Spies*, *supra* at 8.

Facilitating the use of cyber-surveillance tools by a larger group of governments would exacerbate this problem. Not only would increased use of these tools allow increased opportunities for observation and reverse-engineering, but the selection of targets may be less discerning. As noted above, the countries with the technological capability to create

their own tools also have processes like the VEP to take into consideration the risks inherent in using cyber-surveillance, like the risk that a target will detect and weaponize a given surveillance tool. *See supra* at 18-20. Many countries that simply buy a tool from a private company would lack such processes, either because they have not spent the time to develop such processes, or because the risks to their own interests from damage to the cybersecurity ecosystem are much smaller. Accordingly, such countries are more likely to deploy tools against sophisticated targets able to repurpose them in dangerous ways.

In sum, more private cyber-surveillance companies selling more cyber-surveillance tools to more foreign-government clients that could not develop such tools themselves and may exercise less discretion in how they are used means dramatically more opportunities for those tools to fall into the wrong hands and be used nefariously.

C. These increased systemic risks would do extensive damage.

The systemic risks imposed by these increased commercial uses are not minor. One might think that, as soon as one of these tools is used, the underlying vulnerability can always be quickly patched. But

that is not so. Vulnerabilities are not always—or even usually—detected quickly. A recent study found that vulnerabilities remain unknown to their creators for an average of 6.9 years. *See* Ablon & Bogart, *supra* note 4, at 33. But they can, of course, persist much longer than that. In 2018, for example, security researchers identified a zero-day vulnerability in Intel's computer chips that had existed since the mid-1990s. *See* Andy Greenberg, *Triple Meltdown: How So Many Researchers Found a 20-Year-Old Chip Flaw at the Same Time*, Wired (Jan. 7, 2018), https://tinyurl.com/ydbdjfp7. Because these vulnerabilities can be undisclosed—and unpatched—for such a long time, the damage done by a tool falling into the hands of a malicious actor can be extensive.

Even limited use of these tools can cause massive disruption and expense. When an exploited vulnerability is finally identified, a monumental undertaking begins. Damage from these attacks often cascades downstream, with each infected device infecting other devices with which it communicates. Consequently, hundreds or thousands of companies may need to engage in incident response processes and mitigation steps with respect to millions of users. Take the 2017

NotPetya attack, for example. One obvious cost of such an attack is the cost of developing—and implementing—a patch.[12] But that was far from the only cost. When companies realized that they were being targeted, they frantically scrambled to take their devices and systems offline to prevent further spread and damage. *See, e.g.*, *Untold Story*, *supra* note 3. Companies then had to figure out how to repair infected devices—or, if repairs were impossible, to replace them. As illustrated above, the problem is massive: Merck alone had to deal with 30,000 infected computers and 7,500 infected servers. *See supra* at 6. Added to this are the downstream consequences of having systems offline for extended periods of time—business and government closures, delayed vaccine production, etc.

And some of the damage done by cyberattacks can *never* be undone, even after the vulnerability is identified. Once spyware has

[12] In that case, Microsoft actually developed its patch before the attack, because the NSA had warned it of the Shadow Brokers leak. See *Strange Journey*, *supra* at 7. But it takes time for users to update the billions of devices across the globe with software updates containing the patch. See, e.g., Kelly Jackson Higgins, *Unpatched Vulnerabilities the Source of Most Data Breaches*, Dark Reading (April 5, 2018), https://tinyurl.com/y4xat346 ("[M]ost organizations still struggle to keep up with and manage the process of applying software updates.")

been placed on a device, for example, it may continue to surveil the user's activity and report back, even after the vulnerability that first allowed access to the device is patched; the user may have to perform a "factory reset"—removing all personal data and programs from the device to return it in its original, out-of-the-box state—to remove the spyware. *See How to detect spyware to safeguard your privacy?,* Kaspersky Lab, https://tinyurl.com/y679odja (hereinafter "*How to detect spyware*"). But even that may not work. *See, e.g.*, David Murphy, *This New Android Malware Can Survive a Factory Reset*, LifeHacker (Oct. 30, 2019), https://tinyurl.com/yxwjut25. Moreover, users will frequently not know that the spyware was installed, and so will not know to initiate a reset.

Even if there is a way to remove spyware from a device, a hacker will continue to have access to information that it downloaded from the device while the spyware was functioning. This may include credentials (like passwords or account numbers) that allow continued access post-patch. *See, e.g., How to detect spyware*, *supra*. Again, users frequently will not know that their credentials or other information have been compromised.

The damage done by a ransomware, too, may be permanent, as information stored on a given device may be gone forever. *See, e.g.*, *Untold Story*, *supra* note 3 (Merck researcher reported losing more than a decade of research as a result of NotPetya).

When powerful cyber-tools fall into the wrong hands, the damage therefore is extensive and long-lasting. The NotPetya attack in 2017 spread throughout the globe like wildfire, inflicting billions of dollars of damage in a single day. That is just the tip of the iceberg of the damage likely to come if private companies can engage in cyber-surveillance at the behest of governments with impunity.

CONCLUSION

The expansion of sovereign immunity that NSO seeks here would further encourage the burgeoning cyber-surveillance industry to develop, sell, and use tools to exploit vulnerabilities in violation of U.S. law. The resulting proliferation of cyber-surveillance companies would put powerful cyber-tools in the hands of more people than even before. This means more tools stored on unsecure systems vulnerable to hacks, more tools used against sophisticated targets capable of stealing the technology, more cyberattacks, and more resulting damage. The court

should not countenance this result. Private companies should remain subject to liability when they use their cyber-surveillance tools in violation of U.S. law, regardless of who their customers are.

Respectfully Submitted,

GOOGLE LLC

/s/Michael Trinh
Michael Trinh
Counsel for Amicus Google LLC

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/Mark Parris
Mark Parris
Counsel for Amici Curiae Microsoft Corp., Cisco Systems, Inc., GitHub, Inc., LinkedIn Corporation, VMware, Inc., and Internet Association

Dated: December 21, 2020

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): 20-16408

I am the attorney or self-represented party.

This brief contains 5,556 words, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 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 Fed. R. App. P. 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; or
- [ ] 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/*Mark Parris* **Date** December 21, 2020
(use "s/[typed name]" to sign electronically-filed documents)