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

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Carlos Dada, et al.,
Plaintiffs-Appellants

v.

NSO Group Technologies, et al.,
Defendants-Appellees.

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

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF PLAINTIFFS-APPELLANTS AND REVERSAL

Megan Iorio
Chris Baumohl
Maria Villegas Bravo
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
iorio@epic.org

Attorneys for Amicus Curiae

July 22, 2024

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amicus curiae* the Electronic Privacy Information Center states that it has no parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT i

TABLE OF AUTHORITIES iii

INTEREST OF THE *AMICUS CURIAE* 1

SUMMARY OF THE ARGUMENT 2

ARGUMENT 4

I. The United States has an interest in enforcing the CFAA against foreign hackers who attack U.S. computer infrastructure. 4

A. The CFAA's text and legislative history show that the law applies extraterritorially. 5

B. The borderless nature of computer crimes requires the CFAA to apply extraterritorially. 8

II. Spyware attacks undermine user trust in platforms, which is a substantial local interest. 13

A. A significant portion of U.S. users entrust Apple devices and communications networks with their most sensitive personal information. 13

B. Spyware's exploitation of Apple's infrastructure to target Plaintiffs-Appellants transformed trusted devices and networks into tools of unmatched surveillance, harming user trust in this digital infrastructure. 17

III. Individual victim cases are vital to giving the CFAA full effect 24

CONCLUSION 29

CERTIFICATE OF COMPLIANCE 31

CERTIFICATE OF SERVICE 32

TABLE OF AUTHORITIES

Cases

Apple v. NSO Grp. Techs.,
No. 3:21-cv-09078-JD, 2024 WL 215448 (Jan. 23, 2024)..... 28, 29

hiQ Labs, Inc. v. LinkedIn Corp.,
31 F. 4th 1180 (9th Cir. 2022) 6, 28

In re Apple Device Performance Litig.,
347 F. Supp. 3d 434 (N.D. Cal. 2018) 8

Riley v. California,
573 U.S. 373, 403 (2014)..... 15

RJR Nabisco, Inc. v. Eur. Cmty.,
579 U.S. 325 (2016)..... 5

Ryanair DAC v. Booking Holdings Inc.,
No. CV 20-1191-LPS, 2021 WL 7209367 (D. Del. Dec. 27, 2021).... 8

Ryanair DAC v. Expedia Inc.,
No. C17-1789RSL, 2018 WL 3727599 (W.D. Wash.
Aug. 6, 2018)..... 7, 8

United States v. Gasperini,
729 F. App'x 112 (2d. Circ. 2018)..... 7

United States v. Ivanov,
175 F. Supp. 2d 367 (D. Conn. 2001) 7

Van Buren v. United States,
593 U.S. 374 (2021)..... 6, 17

Statutes

Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030 5

§ 1030(e)(2)(B)..... 5

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56 § 814(d)(1), 115 Stat. 272 (codified as amended at 18 U.S.C. § 1030(e)(2)(B)) 8

Other Authorities

Amazon Web Services, *AWS Global Infrastructure Map* (2024) 11

Apple Developer, *Build Trust Through Better Privacy* 21

Apple, *About Apple threat notifications and protecting against mercenary spyware* (Apr. 10, 2024) 29

Apple, *About Lockdown Mode* (Jan. 10, 2024) 28

Apple, *Apple Advances User Security with Powerful New Data Protections* (Dec. 7, 2022) 20, 21

Apple, *iMessage with PQ3: The New State of the Art in Quantum-secure Messaging at Scale* (Feb. 21, 2024) 21

Complaint, *Apple v. NSO Grp. Tech.*, No. No. 3:21-cv-09078 (Nov. 23, 2021) 27, 37

Craig Timberg et al., *On the list: Ten prime ministers, three presidents and a king*, Wash. Post (July 20, 2021) 25

Dana Priest, Craig Timber, & Souad Mekhennet, *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, Wash. Post (July 18, 2021) 35

Danielle Keats Citron & Daniel J. Solove, Privacy Harms, 102 B.U. L. Rev. Online 793, 841–59 (2022) 34

David Sanger et al., *U.S. Blacklists Israeli Firm NSO Group Over Spyware*, N.Y. Times (Nov. 3, 2021) 32

El Salvador journalists sue spyware maker in US court, Associated Press (Nov. 30, 2022) 30

Eric Griffith, *What is Cloud Computing?*, PC Mag. (Feb 15, 2022) 10

Frank Bajak, *Journalists, lawyers and activists hacked with Pegasus spyware in Jordan, forensic prob finds*, Associated Press (Feb. 1, 2024) 26

Google, *Discover our data center locations* (2024) 11

Google, *What is Cloud Computing?* 10

Homeland Security Investigations, *Cybercrime* (Apr. 22, 2024) 14

Indictment, *United States v. Khoroshev*, No. 2:24-cr-00299 (D. N.J. May 02, 2024) 15

Indictment, *United States v. Martins et al.,* No. 17-20238-SHL (W.D. Tenn. Aug. 24, 2017) 16

Indictment, *United States v. Morenets et al.,* No. 18-263 (W.D. Pa. Oct. 03, 2018) 16

Indictment, *United States v. Wu Zhiyong et al.*, No. 1:20-CR046 (N.D. Ga. Jan. 28, 2020) 15

Internet Soc'y, *A Policy Framework for an Open and Trusted Internet: An Approach for Reinforcing Trust in an Open Environment* 6 (Mar. 2017) 19

Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326 (2015) 10, 12

Jonathon W. Penney & Bruce Schneier, *Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group*, 36 Berkeley Tech. L. J. 469 (2021) 13, 14

Katie Benner, David E. Sanger, & Julian E. Burnes, *Israeli Company's Spyware Is Used to Target U.S. Embassy Employees in Africa*, N.Y. Times (Dec. 3, 2021) 28

Kelvin Chan, *Meta fined record $1.3 billion and ordered to stop sending European user data to US*, Associated Press (May 22, 2023) 11

Laura King, *'Cut it into pieces': Jamal Khashoggi's dismemberment was methodically planned, U.N. report says*, L.A. Times (June 19, 2019) 35

Mark Mazzetti, *Biden Acts to Restrict U.S. Government Use of Spyware*, N.Y. Times (Mar. 27, 2023) 32

Mark Mazzetti, Ronen Bergman & Matina Stevis-Gridneff, *How the Global Spyware Industry Spiraled Out of Control*, N.Y. Times (Dec. 8, 2022) 29

Mark Mazzetti, *U.S. Blacklists Two Spyware Firms Run by an Israeli Former General*, N.Y. Times (July 18, 2023) 31

Memorandum, Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion, Off. of Deputy Att'y. Gen. (Jun. 3, 2021) 15

Merlin Delcid, *El Salvador denies responsibility for hacking journalists after report finds Pegasus spyware on their phones*, CNN (Jan. 13, 2022) 31

Meta, *Meta's global data center fleet* (2024) 11

Mobile Operating System Market Shared United States of America, StatCounter 17

Nat'l Intell. Council, *Digital Repression Growing Globally, Threatening Freedoms* (Oct. 31, 2022) 24

Nicole Perlroth, *Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones*, N.Y. Times (Nov. 23, 2021) 30

Off. U.N. High Commissioner for Human Rts., *The Right to Privacy in the Digital Age* (Aug. 4, 2022) 23, 34

Omer Benjakob, *The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware*, Haaretz (Apr. 5, 2022) 26

Piper Sandler, *Piper Sandler Completes 45th Semi-Annual Generation Z Survey of 5,690 U.S. Teens* (Apr. 4, 2023) 18

Ronan Farrow, *A Hacked Newsroom Brings a Spyware Maker to U.S. Court*, New Yorker (Nov. 30, 2022) 31

Ronen Bergman & Patrick Kingsley, *Israeli Spyware Maker Is in Spotlight Amid Reports of Wide Abuses*, N.Y. Times (July 18, 2021) 34

S. Rep. 104-357 (1996) 6, 7

Siena Anstis et al., *The Dangerous Effects of Unregulated Commercial Spyware*, CitizenLab (June 24, 2019) 24

Stephanie Kirchgaessner, *Washington DC-based group targeted in apparent Pegasus hack*, Guardian (Sept. 8, 2023) 27

Tim Starks & Joseph Menn, *Why cybersecurity experts say you should update your iPhone ASAP*, Wash. Post (Sept. 8, 2023) 29

Tripp Mickle, *Smartphone Industry Sputters, the iPhone Expands Its Dominance*, N.Y. Times (Sept. 11, 2023) 17

Vanessa Gera, *Poland's prosecutor general says previous government used spyware against hundreds of people*, Associated Press (Apr. 24, 2024) 27

Whitney Blair Wyckoff, *Poll: American Voters Overwhelmingly Want Privacy, Encryption*, FedScoop (Apr. 18, 2016) 20

INTEREST OF THE *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC advocates for meaningful oversight of invasive surveillance. EPIC is concerned that the district court's analysis would harm U.S. users by undermining trust in U.S. technology platforms and leave spyware victims with no reasonable forum to enforce their rights.

EPIC regularly participates as amicus in this Court and others in cases concerning privacy, surveillance, and the Computer Fraud and Abuse Act (CFAA). *See, e.g.*, Br. of EPIC as Amicus Curiae, *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985 (9th Cir. 2019) (filed Oct. 10, 2017); Br. of EPIC as Amicus Curiae, *hiQ Labs, Inc. v. LinkedIn Corp.*, 141 S. Ct. 2752 (2021) (filed Apr. 13, 2020); Br. of EPIC et al. as Amici Curiae, *Van Buren v. United States*, 593 U.S. 374 (2021) (filed Sept. 3, 2020).[1]

---

[1] All parties consent to the filing of this brief. In accordance with Rule 29, the undersigned states that no party or party's counsel authored this brief in whole or in part nor contributed money intended to fund the preparation of this brief. No outside person contributed money intended to fund the preparation of this brief.

SUMMARY OF THE ARGUMENT

Congress enacted the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, to protect computer infrastructure, devices, and data from hacking and other forms of unauthorized access. In the decades since its enactment, Congress has amended the CFAA several times, notably in 1996 and in 2001, to expand the scope of protected computers to reach the conduct of foreign hackers who compromise the international computer networks that the United States relies upon.

The need to enforce the CFAA extraterritorially has only become more urgent as computer data and infrastructure has become increasingly borderless. Servers in the United States support devices all over the world, from hosting remote applications and data to providing secure communications services like encryption. The United States has an interest in enforcing the CFAA against those who exploit U.S. computer infrastructure, no matter where the hackers or the victims are located at the time of the hack.

The district court failed to appreciate the substantial local interest in applying the CFAA to spyware that exploits U.S. technology platforms and infrastructure that a broad swath of the American public

relies on. Spyware attacks do not just affect the victims; they undermine user trust in the platforms themselves, a harm which directly impacts California residents. A significant portion of Americans entrust Apple devices and communications networks with their sensitive personal information. The exploitation of Apple's encrypted infrastructure by spyware firms like NSO Group transforms entrusted devices and networks into tools of surveillance, eroding all users' trust that their devices and data are secure from attack.

While technology companies have brought lawsuits arising out of the use of Defendants'-Appellees' spyware, individual victim cases—such as this case—are vital for giving the CFAA full effect. One of the CFAA's core purposes is to protect people from hackers. Therefore, if anyone should be able to sue under the CFAA, it is the victims of hacking.

Individual and corporate victim cases are complementary, not mutually exclusive. Individual and corporate cases focus on different harms, and individuals are better able to represent the privacy and trust harms that spyware causes than corporations. Indeed, in other CFAA cases, courts have failed to fully appreciate the significance of

user privacy interests when adjudicating disputes between corporate parties.

Failing to adequately enforce the CFAA against foreign hackers like NSO Group undermines the public trust in Apple's infrastructure upon which most Americans rely. While lawsuits by Apple and WhatsApp are ongoing, they are insufficient to fully and adequately enforcing the CFAA to protect U.S. users from spyware.

ARGUMENT

I. THE UNITED STATES HAS AN INTEREST IN ENFORCING THE CFAA AGAINST FOREIGN HACKERS WHO ATTACK U.S. COMPUTER INFRASTRUCTURE.

Congress explicitly intended the CFAA to apply extraterritorially. To give the CFAA full effect, the law must be enforced against foreign hackers who exploit computer infrastructure that the U.S. relies upon. In the internet age, computer crimes are borderless because computer access, information and infrastructure are distributed across borders. The United States has an interest in enforcing the CFAA when U.S. computer infrastructure is implicated, no matter where the hackers or victims were located at the time of the hack.

A. The CFAA's text and legislative history show that the law applies extraterritorially.

The text and history of the CFAA "gives a clear, affirmative indication that it applies extraterritorially." *RJR Nabisco, Inc. v. Eur. Cmty.*, 579 U.S. 325, 337 (2016). The statute's plain language protects against intrusions into computers both inside and outside the United States. The legislative history also shows Congress's clear intent that the CFAA be used against foreign hackers.

The plain language of the CFAA indicates its extraterritorial reach. The law prohibits anyone from knowingly or intentionally accessing a "protected computer" without or in excess of authorization. 18 U.S.C. § 1030. "Protected computer" is defined expansively to include any computer that is "used in or affect[s] interstate or *foreign* commerce or communication, including a computer located *outside the United States* that is used in a manner than affects interstate or *foreign* commerce or communications in the United States." 18 U.S.C. § 1030(e)(2)(B) (emphasis added). Courts have interpreted the term "protected computer" broadly to include all computers that connect to the internet. *See, e.g.*, *Van Buren v. United States*, 593 U.S. 374, 379

(2021); *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F. 4th 1180, 1195 (9th Cir. 2022). The references to "foreign commerce and communication," as well as computers "outside the United States," in the definition of protected computer clearly indicate Congress's intent that the CFAA apply extraterritorially.

First, Congress added "used in or affecting . . . foreign commerce or communications" to close a previous gap in coverage for foreign hackers. The Senate Report for the 1996 amendments noted that the previous version of the CFAA "omitted . . . computers used in foreign communications or commerce, despite the fact that hackers are often foreign-based." S. Rep. 104-357, at 4 (1996) [Hereinafter, the "Senate Report"]. The Report pointed to two cases where hackers based in the United Kingdom and Argentina hacked into strategically important computers. *Id.* at 4-5. The expansion of subsection 1030(a)(2)(C) to "any protected computers" was also "intended to protect against the interstate or *foreign* theft of information by computer." *Id.* at 7. And that is exactly how courts have interpreted it since: as a "clear" indication that Congress intended the CFAA to apply to international cybercrimes. *United States v. Ivanov*, 175 F. Supp. 2d 367, 374 (D.

Conn. 2001); *see also United States v. Gasperini*, 729 F. App'x 112, 114 (2d. Circ. 2018) ("There is a strong argument that § 1030(a)(2) applies extraterritorially.").

Congress's decision in 2001 to further expand the definition of "protected computer" to include a computer "*outside of the United States* that is used in a manner that affects interstate or foreign commerce or communication of the United States" solidified the CFAA's extraterritorial reach. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56 § 814(d)(1), 115 Stat. 272 (codified as amended at 18 U.S.C. § 1030(e)(2)(B)) (emphasis added). Courts have repeatedly recognized that including computers "outside the United States" within the definition of protected computer "is as clear an indication [that the CFAA applies extraterritorially] as possible short of saying 'this law applies abroad.'" *Ryanair DAC v. Expedia Inc.*, No. C17-1789RSL, 2018 WL 3727599, at *2 (W.D. Wash. Aug. 6, 2018) (quoting *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 265 (2010)); *Ryanair DAC v. Booking Holdings Inc.*, No. CV 20-1191-LPS,

2021 WL 7209367, at *7 (D. Del. Dec. 27, 2021); *In re Apple Device Performance Litig.*, 347 F. Supp. 3d 434, 448 (N.D. Cal. 2018).

The text and history of the CFAA clearly indicate that Congress intended the statute to apply extraterritorially. To *Amicus's* knowledge, no court has ever found that the CFAA does *not* apply extraterritorially.

B. The borderless nature of computer crimes requires the CFAA to apply extraterritorially.

"It makes sense that the CFAA extends protection to computers outside the United States" because of the borderless nature of computer crimes in the internet age. *Expedia,* 2018 WL 3727599, at *3. The internet makes it just as easy for a foreign hacker as a domestic hacker to attack U.S. computer infrastructure. U.S. computer infrastructure also supports cloud computing and other services worldwide, which means that U.S. computer infrastructure can be attacked even when the hacker and individual victim are located abroad. Enforcing the CFAA against these hackers helps protect U.S. interests in the security of this infrastructure. Computer crimes laws must be flexible in terms of territoriality to properly address the security threats of today.

Computers today are, in many ways, borderless. Cloud computing has made it so that much of the data and software that people access from their devices are stored not on the devices but on remote servers, often referred to as "the cloud." *See* Eric Griffith, *What is Cloud Computing?*, PC Mag. (Feb 15, 2022);[2] Google, *What is Cloud Computing?*.[3] The cloud itself is not a single place, and data located on the cloud may be copied onto multiple servers at different locations to protect against data loss from server malfunctions. Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 368 (2015). Multinational companies like Meta, Google, and Amazon have servers all over the world. Meta, *Meta's global data center fleet* (2024);[4] Google, *Discover our data center locations* (2024);[5] Amazon Web Services, *AWS Global Infrastructure Map* (2024).[6] U.S. companies often process and store foreign users' data in the United States. *See e.g.* Kelvin Chan,

---

[2] https://www.pcmag.com/how-to/what-is-cloud-computing.
[3] https://cloud.google.com/learn/what-is-cloud-computing (last accessed June 22, 2024).
[4] https://datacenters.atmeta.com/all-locations/.
[5] https://www.google.com/about/datacenters/locations/.
[6] https://aws.amazon.com/about-aws/global-infrastructure/.

Meta fined record $1.3 billion and ordered to stop sending European user data to US, Associated Press (May 22, 2023).[7]

Because devices in foreign countries are often dependent on U.S. computer systems for cloud computing services, foreign hackers who attack foreign devices can, in the process, access or otherwise affect U.S. computers. Cloud computing has thus "call[ed] into question the normative significance of longstanding distinctions between what is territorial and what is extraterritorial." Daskal, *supra* at 330. When foreign devices are hacked and U.S. cloud services are accessed during the hack, or used as a staging ground for the attack, U.S. interests are implicated, and the CFAA should apply.

Encrypted networks also span borders, and when these networks are exploited to hack into a target's device, all of the computers in the network are compromised, not just the target's device. Encrypted communications networks protect the security of messages while they are in transit by making it so that only the sender and recipient can

---

[7] https://apnews.com/article/meta-facebook-data-privacy-fine-europe-9aa912200226c3d53aa293dca8968f84.

read them. Jonathon W. Penney & Bruce Schneier, *Platforms, Encryption, and the CFAA: The Case of WhatsApp v. NSO Group*, 36 Berkeley Tech. L. J. 469, 471 (2021). The users of an encrypted network depend on the security of the encrypted network provider's computers for this service. *Id.* at 489–91. All of these devices—the individual sending and receiving devices, along with the encryption provider's computers—together form the encrypted network. *Id.* at 486, 492–93. Becausethe encryption provider's computers may be in a different country than the sender and receiver's devices—which themselves may be in separate countries—encryption networks can span borders. Exploits of encrypted networks are attacks on the whole network, and so also span borders. *Id.* at 491–92, 498. The U.S. has an interest in enforcing the CFAA when foreign hackers attack foreign victims through U.S. encryption networks because such conduct threatens critical U.S. computer infrastructure upon which a large portion of the U.S. population relies.

U.S. law enforcement recognizes the borderless nature of computer crimes and uses its authority under the CFAA to prosecute foreign hackers who attack U.S. computer infrastructure. The

Department of Homeland Security's definition of cybercrime explicitly refers to cybercrime's "borderless" nature. Homeland Security Investigations, *Cybercrime* (Apr. 22, 2024).[8] According to the Deputy Attorney General, ransomware attacks and digital extortion schemes are of particular concern to the U.S. when they are "conducted by transnational criminal actors, spread without regard to geographic borders [which] thrive on the abuse of online digital and financial infrastructure." Memorandum, Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion, Off. of Deputy Att'y. Gen. (Jun. 3, 2021).[9] The Department of Justice also regularly prosecutes individuals for exploiting U.S. infrastructure to obtain sensitive information regardless of where the defendant is located. S*ee* Indictment, *United States v. Khoroshev*, No. 2:24-cr-00299 (D. N.J. May 02, 2024); Indictment, *United States v. Wu Zhiyong et al.*, No. 1:20-CR046 (N.D. Ga. Jan. 28, 2020); Indictment, *United States v. Morenet*s

[8] https://www.dhs.gov/hsi/investigate/cybercrime.
[9] https://www.justice.gov/opa/press-release/file/1402001/dl.

et al., No. 18-263 (W.D. Pa. Oct. 03, 2018); Indictment, *United States v. Martins et al.*, No. 17-20238-SHL (W.D. Tenn. Aug. 24, 2017).

Cybercrime cannot be addressed only within the borders of the United States. The CFAA applies extraterritorially to allow the United States to protect important U.S. computer infrastructure in a comprehensive manner.

II. SPYWARE ATTACKS UNDERMINE USER TRUST IN PLATFORMS, WHICH IS A SUBSTANTIAL LOCAL INTEREST.

The public has a robust interest in ensuring the security of encrypted networks upon which a significant portion of Americans rely. Spyware attacks, such as those alleged by Plaintiffs-Appellants, not only affect individual victims but undermine general user trust in platforms themselves. Courts must protect these interests by enforcing existing protections against unauthorized intrusion into encrypted networks and devices.

A. A significant portion of U.S. users entrust Apple devices and communications networks with their most sensitive personal information.

A significant portion of Americans—including the vast majority of young Americans—trust Apple's encrypted infrastructure to safeguard

their most sensitive information from unauthorized outside access. Apple accounts for more than half of all devices sold in the United States. *Mobile Operating System Market Shared United States of America*, StatCounter.[10] iPhones account for more than half of all smartphones sold in the United States. Tripp Mickle, *Smartphone Industry Sputters, the iPhone Expands Its Dominance*, N.Y. Times (Sept. 11, 2023).[11] American consumers' reliance upon Apple devices is growing: nearly 90 percent of teenagers own an iPhone. Piper Sandler, *Piper Sandler Completes 45th Semi-Annual Generation Z Survey of 5,690 U.S. Teens* (Apr. 4, 2023).[12] American journalists, activists, and government officials all rely on Apple devices and networks in their personal and professional capacities.

People trust Apple's encryption to protect the sensitive information transferred along Apple's networks and stored on their

---

[10] https://gs.statcounter.com/os-market-share/mobile/united-states-of-america (last visited June 3, 2024).
[11] https://www.nytimes.com/2023/09/11/technology/apple-iphone-17.html.
[12] https://www.pipersandler.com/news/piper-sandler-completes-45th-semi-annual-generation-z-survey-5690-us-teens.

devices and servers. Smartphone infrastructure—including Apple's—stores users' most sensitive information. *See Riley v. California*, 573 U.S. 373, 403 (2014) (finding that modern cell phones hold for many Americans "the privacies of life") (quoting *Boyd v. United States*, 116 U.S. 616, 625 (1886)). Encryption and other similar technologies in turn build user trust in encrypted networks and devices because they:

> enable Internet users to communicate privately (confidentiality), know who they are communicating with (authentication), know that the information they are sending or receiving has not been altered in transit (integrity), to restrict access to their data or communications (authorization), and know whether their device or technology has been tampered with (tamper detection and resistance).

Internet Soc'y, *A Policy Framework for an Open and Trusted Internet: An Approach for Reinforcing Trust in an Open Environment* 6 (Mar. 2017).[13] U.S. users want the protections encryption offers, voicing overwhelming support for the adoption of encryption technology to keep their information secure and private. *See* Whitney Blair Wyckoff, *Poll:*

---

[13] https://www.internetsociety.org/wp-content/uploads/2017/08/bp-Trust-20170314-en.pdf.

American Voters Overwhelmingly Want Privacy, Encryption, FedScoop (Apr. 18, 2016).[14]

Understanding the interest users have in safeguarding their privacy, Apple markets its devices and infrastructure as secure and private, with encryption a key feature. *See* Apple, *Apple Advances User Security with Powerful New Data Protections* (Dec. 7, 2022) (highlighting Apple's "best-in-class device encryption").[15] Apple has continued to roll out encryption across its networks in recent years. *See id.*; *see also* Apple, *iMessage with PQ3: The New State of the Art in Quantum-secure Messaging at Scale* (Feb. 21, 2024).[16] Apple has regularly touted its efforts to "[b]uild trust through better privacy[,]" including through security measures like encryption. *See* Apple Developer, *Build Trust Through Better Privacy*.[17] As a result, Apple users trust Apple to not only have its gates up, but to have those gates

---

[14] https://fedscoop.com/survey-most-americans-want-data-on-their-phone-to-stay-private/.
[15] https://www.apple.com/newsroom/2022/12/apple-advances-user-security-with-powerful-new-data-protections/.
[16] https://security.apple.com/blog/imessage-pq3/.
[17] https://developer.apple.com/videos/play/wwdc2020/10676/.

be high. *Cf. Van Buren v. United States*, 593 U.S. 374, 390 (2021). Threats to this trust intimately affect the millions of Americans who rely on Apple's encryption.

B. Spyware's exploitation of Apple's infrastructure to target Plaintiffs-Appellants transformed trusted devices and networks into tools of unmatched surveillance, harming to user trust in this digital infrastructure.

Exploits of encrypted networks, such as the spyware attacks alleged here, are especially damaging to user trust because people rely on these networks to carry very sensitive information and because spyware necessarily endangers *all* users of Apple's infrastructure, not just the ones targeted by a specific attack.

As encryption has grown, spyware tools—such as that of Defendants-Appellees—have proliferated. Recognizing that more and more users rely on encrypted communications systems and services that store data in encrypted form, spyware manufacturers use encryption exploits to gain unauthorized and surreptitious access to victims' devices. Through the victim's device, a hacker can gain access to everything on the device (including communications, photos, and videos), information accessible through mobile applications and remote

storage (such as financial information, work documents, and health data), and information that can be inferred from these mobile applications (e.g., sexual orientation, political affiliation, and religious practices). *See* Off. U.N. High Comm'r for Human Rts., *The Right to Privacy in the Digital Age* 3 (Aug. 4, 2022).[18] Hackers can also use their access to the victim's device to capture new information—in real time—through the camera, microphone, or other device features, essentially converting the device into a bug that goes everywhere with the victim.

By transforming encrypted devices and networks into tools of unmatched surveillance, spyware attacks severely degrade user trust in encrypted infrastructure. Spyware enables real-time monitoring of victims, "effectively turning most smartphones into 24-hour surveillance devices." *See* Off. U.N. High Comm'r for Human Rts., *The Right to Privacy in the Digital Age* 3 (Aug. 4, 2022). Using this unauthorized access, spyware clients can engage in invasive surveillance, digital repression, and even carry out physical violence and assassinations. *See* Nat'l Intell. Council, *Digital Repression*

---

[18] https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.

Growing Globally, Threatening Freedoms (Oct. 31, 2022);[19] Siena Anstis et al., *The Dangerous Effects of Unregulated Commercial Spyware*, CitizenLab (June 24, 2019).[20]

Spyware attacks on specific victims—in this case, the Plaintiffs-Appellants—rely on exploits designed to target *all* users of Apple's infrastructure, and thus impacts a significant portion of the U.S. public. Spyware is designed to circumvent software that *all* Apple users rely on, including Apple's security protections, the encryption of Apple's infrastructure, and the security infrastructure of mobile applications—like encrypted messaging apps. Indeed, as of July 2021, Defendants-Appellees were "able to remotely and covertly compromise all recent iPhone models and versions of Apple's mobile operating system." ER-026 (Am. Compl. ¶ 45).

Although these exploits may be deployed only against specific targets, they work against any person's device and have been deployed

---

[19] https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-Assessment-Digital-Repression-Growing-April2023.pdf.
[20] https://citizenlab.ca/2019/06/the-dangerous-effects-of-unregulated-commercial-spyware/.

widely. A list of 50,000 suspected targets was leaked in 2021 and there have been hundreds of confirmed infections using Defendants'-Appellees' spyware since then. *See* Craig Timberg et al., *On the list: Ten prime ministers, three presidents and a king*, Wash. Post (July 20, 2021);[21] Omer Benjakob, *The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware*, Haaretz (Apr. 5, 2022).[22] This includes hundreds of journalists, lawyers, activists, and other civil society figures across dozens of countries. *See* Frank Bajak, *Journalists, lawyers and activists hacked with Pegasus spyware in Jordan, forensic prob finds*, Associated Press (Feb. 1, 2024);[23] Vanessa Gera, *Poland's prosecutor general says previous government used spyware against hundreds of people*, Associated Press (Apr. 24, 2024).[24] Further, although NSO Group claims its spyware cannot be used to conduct

---

[21] https://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/.
[22] https://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000.
[23] https://apnews.com/article/jordan-hacking-pegasus-spyware-nso-group-99b0b1e4ee256e0b4df055f926349a43.
[24] https://apnews.com/article/poland-spyware-pegasus-nso-group-israel-413bb3cb27daac011d52b524c6d16160.

surveillance within the United States, U.S. citizens have been surveilled via NSO Group spyware installed on devices registered to non-U.S. phone numbers, both within and outside of the United States. *See* Complaint at 4, *Apple v. NSO Grp. Tech.*, No. No. 3:21-cv-09078 (Nov. 23, 2021); Stephanie Kirchgaessner, *Washington DC-based group targeted in apparent Pegasus hack*, Guardian (Sept. 8, 2023);[25] Katie Benner, David E. Sanger, & Julian E. Burnes, *Israeli Company's Spyware Is Used to Target U.S. Embassy Employees in Africa*, N.Y. Times (Dec. 3, 2021).[26]

Apple treats spyware attacks as threats to *all* users and urges them to take steps to protect themselves from such attacks. Apple has released new security features to all users, including its new Lockdown Mode, a configuration option for individuals at particular risk of being targeted by spyware. *See* Apple, *About Lockdown Mode* (Jan. 10, 2024).[27] Apple and outside experts also regularly update guidance for all

---

[25] https://www.theguardian.com/us-news/2023/sep/08/pegasus-hack-washington-dc-group-nso.
[26] https://www.nytimes.com/2021/12/03/us/politics/phone-hack-nso-group-israel-uganda.html.
[27] https://support.apple.com/en-us/105120.

users on how to protect themselves against spyware. *See* Apple, *About Apple threat notifications and protecting against mercenary spyware* (Apr. 10, 2024);[28] Tim Starks & Joseph Menn, *Why cybersecurity experts say you should update your iPhone ASAP*, Wash. Post (Sept. 8, 2023).[29]

U.S. users are keenly aware of the risks spyware poses to their own devices because of the very public nature of spyware attacks. Major U.S. outlets have devoted significant coverage to the attacks and their consequences. *See* Mark Mazzetti, Ronen Bergman & Matina Stevis-Gridneff, *How the Global Spyware Industry Spiraled Out of Control*, N.Y. Times (Dec. 8, 2022);[30] Nicole Perlroth, *Apple Sues Israeli Spyware Maker, Seeking to Block Its Access to iPhones*, N.Y. Times (Nov. 23, 2021).[31] This includes coverage of Plaintiffs'-Appellants' own case. *See El Salvador journalists sue spyware maker in US court*, Associated

---

[28] https://support.apple.com/en-us/102174.
[29] https://www.washingtonpost.com/politics/2023/09/08/apple-issues-software-updates-after-spyware-discoveries/.
[30] https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html
[31] https://www.nytimes.com/2021/11/23/technology/apple-nso-group-lawsuit.html.

Press (Nov. 30, 2022);[32] Ronan Farrow, *A Hacked Newsroom Brings a Spyware Maker to U.S. Court*, New Yorker (Nov. 30, 2022);[33] Merlin Delcid, *El Salvador denies responsibility for hacking journalists after report finds Pegasus spyware on their phones*, CNN (Jan. 13, 2022).[34] The U.S. government's attempts to combat mercenary spyware, including spyware developed by NSO Group, has also raised the visibility of these harms among U.S. users. *See* Mark Mazzetti, *U.S. Blacklists Two Spyware Firms Run by an Israeli Former General*, N.Y. Times (July 18, 2023);[35] David Sanger et al., *U.S. Blacklists Israeli Firm NSO Group Over Spyware*, N.Y. Times (Nov. 3, 2021);[36] Mark Mazzetti, *Biden Acts to Restrict U.S. Government Use of Spyware*, N.Y. Times

---

[32] https://apnews.com/article/technology-business-canada-israel-middle-east-1b16abed6e33242c72e2bd07a28cc075.
[33] https://www.newyorker.com/news/news-desk/a-hacked-newsroom-brings-a-spyware-maker-to-us-court-pegasus.
[34] https://www.cnn.com/2022/01/13/americas/el-salvador-pegasus-spyware-intl/index.html.
[35] https://www.nytimes.com/2023/07/18/us/politics/spyware-blacklist-israel-us.html.
[36] https://www.nytimes.com/2021/11/03/business/nso-group-spyware-blacklist.html.

(Mar. 27, 2023).[37] Given the very public nature of these widespread attacks, users in the United States, as well as U.S. users outside the country, such as government officials, members of the military, and others, all have a well-founded reason to believe their devices may be targeted through the use of spyware.

III. INDIVIDUAL VICTIM CASES ARE VITAL TO GIVING THE CFAA FULL EFFECT.

Lawsuits by individual victims are at the heart of the CFAA and are vital to giving the statute full effect. Individual and corporate suits focus on different types of harm. Corporate and individual victim suits are thus complementary, and hearing both types of cases ensures that the CFAA protects against the full range of harms caused by hacking. Defendants'-Appellants' argument that corporate and individual victims' suits are mutually exclusive and that corporations are the proper plaintiffs contradict arguments they made in the corporate suits and are part of a self-serving strategy to evade all legal accountability in U.S. courts.

---

[37] https://www.nytimes.com/2023/03/27/us/politics/biden-spyware-executive-order.html.

Individual and corporate victim suits are complementary, not mutually exclusive, because they protect against different types of harm. Individual victim cases underscore the harms spyware causes people, including physical harms, reputational harms, psychological harms, economic harms, and autonomy harms, including lack of control and chilling effects. See Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. Rev. Online 793, 841–59 (2022) (mapping out a typology of privacy harms).[38] Spyware attacks also seriously interfere with a wide swath of other related rights, including media freedom, freedom of expression, and freedom of association. See Off. U.N. High Commissioner for Human Rts., *The Right to Privacy in the Digital Age* 4 (Aug. 4, 2022).[39] Repressive government authorities have reportedly used Defendants'-Appellees' spyware to target hundreds of journalists, activists, and political dissidents. *See* Ronen Bergman & Patrick Kingsley, *Israeli Spyware Maker Is in Spotlight Amid Reports of*

[38] https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
[39] https://documents.un.org/doc/undoc/gen/g22/442/29/pdf/g2244229.pdf.

Wide Abuses, N.Y. Times (July 18, 2021).[40] Officials from Saudi Arabia, for example, used spyware to surveil individuals close to journalist Jamal Khashoggi. *See* Dana Priest, Craig Timber, & Souad Mekhennet, *Private Israeli spyware used to hack cellphones of journalists, activists worldwide*, Wash. Post (July 18, 2021).[41] Saudi agents then lured Khashoggi to the Saudi embassy in Turkey, murdered him, and dismembered his body. *See* Laura King, *'Cut it into pieces': Jamal Khashoggi's dismemberment was methodically planned, U.N. report says*, L.A. Times (June 19, 2019).[42] Finally, as noted above, spyware attacks degrade user trust in the digital infrastructure upon which we all rely by turning encrypted devices and networks into tools of invasive and abusive surveillance.

Corporate CFAA suits protect different interests. Although some corporate plaintiffs have brought lawsuits arising out of spyware

---

[40] https://www.nytimes.com/2021/07/18/world/middleeast/israel-nso-pegasus-spyware.html.
[41] https://www.washingtonpost.com/investigations/interactive/2021/nso-spyware-pegasus-cellphones/.
[42] https://www.latimes.com/world/la-fg-saudi-arabia-jamal-khashoggi-un-investigation-20190619-story.html.

attacks on their users, these companies' suits focus more on harms to the corporation and only indirectly address privacy and trust harms to users. For example, in its suit, Apple claims it was forced to "incur costs and to devote personnel, resources, and time to identifying and investigating [NSO's] attacks and exploits, developing and deploying security patches and software upgrades; communicating with Apple personnel and users regarding such attacks, exploits, patches, and upgrades, increasing security measures to detect and prevent future attacks; and assessing and responding to legal exposure." Compl. at 7, *Apple v. NSO Grp. Tech.*, No. 3:21-cv-09078 (Nov. 23, 2021). Further, Apple refers to loss of "goodwill" among its users as a result of these spyware attacks. *See id.* at 4. This goodwill is the result of users' *trust* in Apple to keep its most sensitive information secure. Apple is certainly motivated to protect its users—and thus its bottom line—from spyware exploiting its infrastructure. However, Apple cannot fully represent the interests of Apple device users who have experienced separate, direct harms—harms that the CFAA was enacted to protect against.

California residents, and the potential juror pool in this case, are more likely to identify with the harms caused to individual victims than corporate plaintiffs, which underscores the local interest in hearing the individual as well as the corporate suits. And while the corporations might try to represent the interests of their users in their suits, courts have not taken individual interests seriously enough in some CFAA cases when represented by corporate plaintiffs. *See, e.g., hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F. 4th 1180, 1189–90 (9th Cir. 2022) (concluding that LinkedIn users' interests in privacy were outweighed by hiQ's interest in continuing business).

Defendants-Appellants' argument in the present case that U.S. courts don't need to hear individual victim cases because Apple's corporate suit is sufficient is part of a self-serving strategy to avoid all legal accountability in U.S. courts. In response to cases brought by Apple and WhatsApp, Defendants-Appellants have argued the exact opposite—that the proper plaintiffs in a CFAA suit are the individual victims, not the corporations whose infrastructure was hacked. *See Apple v. NSO Grp. Techs.*, No. 3:21-cv-09078-JD, 2024 WL 215448, at *4 (N.D. Cal. Jan. 23, 2024); Mot. to Dismiss at 22–23, *WhatsApp v. NSO*

Grp. Techs., No. 4:19-cv-07123-PJH (N.D. Cal.) (filed Apr. 2, 2020). In doing so, Defendants-Appellants essentially seek to turn the CFAA's protection of complementary—but distinct—interests of individual and corporate victims on its head by creating a Catch-22 in which neither individual victims nor corporate victims can sue, allowing Defendants-Appellants to evade any liability in U.S. courts.

CONCLUSION

Plaintiffs-Appellants allege that their devices were targeted by spyware, endangering the very rights that individual CFAA suits are meant to protect. They allege that this spyware essentially turned their devices into tools of surveillance by exploiting important U.S. computer infrastructure, allowing a repressive government retaliating against them for doing their jobs as journalists. There is little doubt that people across the United States—including in California—have an interest in U.S. courts hearing this case. Defendants'-Appellants' spyware undermines *everyone's* trust in encryption and in their own devices. Spyware has a particularly damaging effect on those most likely to be targeted by such attacks, like activists and journalists.

For the foregoing reasons, EPIC respectfully urges the Court to reverse the district court's order granting NSO Group's motion to dismiss on *forum non conveniens* grounds.

Date: July 22, 2024

/s/ Megan Iorio
Megan Iorio
Chris Baumohl
Maria Villegas Bravo
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae Electronic Privacy Information Center

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

This brief contains 4,815 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/ Megan Iorio* **Date:** July 22, 2024

CERTIFICATE OF SERVICE

I certify that on July 22, 2024, this brief was e-filed through the ACMS System of the U.S. Court of Appeals for the Ninth Circuit. I certify that all participants in the case are registered ACMS users and that service will be accomplished by the ACMS system.

Date: July 22, 2024

/s/ Megan Iorio
Megan Iorio
Chris Baumohl
Maria Villegas Bravo
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center