NO. 21-16233 - lead, 21-35612

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

FORBES MEDIA LLC and THOMAS BREWSTER,

PLAINTIFFS-APPELLANTS,

v.

UNITED STATES OF AMERICA,

DEFENDANT- APPELLEE

On Appeal from the United States District Court
District for Northern California, Oakland
21-mc-80017-PJH

Hon. Phyllis J. Hamilton, Senior District Judge

BRIEF OF AMICI CURIAE THE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA, AND RIANA PFEFFERKORN IN SUPPORT OF PLAINTIFFS-APPELLANTS AND REVERSAL

Aaron Mackey
Counsel of Record
Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: amackey@eff.org
Tel.: (415) 436-9333
Fax: (415) 436-9993

Counsel for amici curiae

Additional Counsel listed on next page.

Brett Max Kaufman
AMERICAN CIVIL LIBERTIES FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Email: bkaufman@aclu.org
Tel.: (212) 549-2603

Jacob A. Snow
ACLU FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Email: jsnow@aclunc.org
Tel.: (415) 621-2493

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES FOUNDATION
39 Drumm Street
San Francisco, CA 94103
Email: jgranick@aclu.org
Tel.: (415) 343-0758

Riana Pfefferkorn
STANFORD INTERNET OBSERVATORY
616 Jane Stanford Way
Stanford, CA 94305
Email: riana@stanford.edu
Tel.: (650) 724-6814

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amici state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: January 10, 2022

By: /s/ *Aaron Mackey*
Aaron Mackey

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST OF AMICI[1]

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 38,000 dues-paying members that has worked for 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. EFF advocates for Internet users' privacy and frequently seeks access to public records reflecting law enforcement surveillance by litigating Freedom of Information Act ("FOIA") requests and petitioning state and federal courts to unseal judicial records. *See, e.g.,* Brief for Electronic Frontier Foundation et al. as Amici Curiae supporting Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402); *EFF v. San Bernardino County Superior Court*, No. CIVDS1930054 (San Bernardino Sup. Ct. Oct. 8, 2019) (seeking to unseal search warrant materials reflecting law enforcement's use of cell-site simulators).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation's civil rights laws. The ACLU of Northern California is a state affiliate of the national ACLU. The ACLU has frequently appeared before courts, including this one, throughout the country in First

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amici certify that no person or entity, other than amici curiae, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. The parties have consented to the filing of this brief.

Amendment cases.

Riana Pfefferkorn is a Research Scholar at the Stanford Internet Observatory, joining this brief in her personal capacity. She studies novel forms of electronic surveillance by law enforcement, using research methods that include filing FOIA requests and petitioning federal courts to unseal judicial records. *See, e.g.*, Brief for the Electronic Frontier Foundation and Riana Pfefferkorn as Amicus Curiae supporting Petitioners-Appellants, *In re Leopold*, 964 F.3d 1121 (D.C. Cir. 2020) (No. 18-5276); *In re Granick*, 388 F. Supp. 3d 1107 (N.D. Cal. 2019 (denying request to unseal district court's sealed docket of post-investigation surveillance matters).

INTRODUCTION

In December 2019, the FBI sought a court order under the All Writs Act ("AWA") to require Sabre, a data broker that amasses details on the airline flights of more than a billion people,[2] to track—in real time and for six months—the prospective location and movements of a person subject to an arrest warrant.[3] The

[2] *Sabre – Powering the Travel Industry*, Sabre (April 23, 2013), https://www.sabre.com/insights/sabre-holdings-powering-the-travel-industry/.

[3] Thomas Brewster, *The FBI Is Secretly Using A $2 Billion Travel Company As A Global Surveillance Tool*, Forbes (July 16, 2020), https://www.forbes.com/sites/thomasbrewster/2020/07/16/the-fbi-is-secretly-using-a-2-billion-company-for-global-travel-surveillance--the-us-could-do-the-same-to-track-covid-19/?sh=68dc01b357eb ("Brewster, *Global Surveillance Tool*").

AWA is not a surveillance statute. Instead, it allows federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). AWA requests and orders are not subject to reporting requirements like those for federal wiretap orders, nor are they subject to the rules governing search warrants. And as this case shows, authorities routinely file AWA requests and orders under seal. These requests remain secret, often indefinitely, much like many other non-warrant surveillance applications made by law enforcement.

The public has a legitimate interest in seeing the court's legal conclusions, and any related legal justification by law enforcement, that authorized tracking a person's movements in real time without a search warrant. Yet the secrecy surrounding the court records at issue here makes it impossible for the public—and Congress—to understand the judiciary's interpretation of the AWA. The secrecy violates the public's rights of access to judicial records and inhibits Congress from exercising oversight over law enforcement's activities reflected in those records. This case highlights the need for public access to records documenting how law enforcement uses novel interpretations of laws to engage in invasive surveillance, particularly where, as here, a court seal shields legal analysis from public scrutiny and where, as here, the data sought reflects intensely private details of people's lives.

The lack of transparency in this case is of a piece with the broad, endemic secrecy surrounding law enforcement requests for people's private data—data that is frequently obtained without a warrant under statutes such as the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, and the Pen Register Act ("PRA"), 18 U.S.C. §§ 3121-3127. In district courts around the country, these court orders, their related court filings (applications, supporting affidavits, etc.), and often the case docket sheets themselves, largely remain under seal indefinitely. Although sealing these court records initially may be justified to protect the secrecy of an active investigation, the records typically stay sealed well after the underlying investigation is over, long past any need for continued secrecy.

In this case, unsealing is necessary so that the public can understand the nature of the government's AWA requests for people's private location data, particularly because Sabre appears to be one of a handful of data brokers that amasses these volumes of people's travels without travelers' knowledge or consent.

More broadly, greater public disclosure of similar law enforcement requests would promote greater accountability and oversight by both the public and our elected representatives. Laws passed by Congress and the Fourth Amendment reflect our society's judgment on what limits we place on law enforcement's ability to comb through our data—data that often reflects the most intimate details

of our lives. Perpetual sealing of the legal reasoning permitting law enforcement to use the AWA to obtain prospective real-time tracking short-circuits the public's ability to ensure that law enforcement is adhering to those laws and the Constitution.

ARGUMENT

I. PUBLIC DISCLOSURE OF THE JUDICIAL RECORDS THAT FORBES MEDIA SEEKS IS ESSENTIAL TO UNDERSTAND THE LEGAL BASIS AUTHORIZING LAW ENFORCEMENT TO OBTAIN INTENSELY PERSONAL DETAILS ABOUT PEOPLE WITHOUT WARRANTS.

At a time when nearly everyone relies on private service providers for nearly everything—from talking to friends, to organizing events, booking travel, storing photographs, shopping, and running businesses—it is essential that the public know how and under what conditions courts authorize the government to access our personal information held by those providers. Before the development of electronic communication and digital services, most of our communications and other interactions left few to no records. And even when those communications or interactions did leave records, the volume paled in comparison to the vast digital ocean of data created today.

As new technologies become ever more embedded into people's everyday lives, providing users with innovative ways to communicate, and making their lives easier, they generate massive amounts of data. The Supreme Court has

repeatedly recognized this reality. *See, e.g.*, *Riley v. California*, 573 U.S. 373, 394 (2014) (explaining that while "a photograph or two of loved ones tucked into a wallet" says something about a person, . . . they reveal nothing close to "[t]he sum of an individual's private life [that] can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions" that are recorded and stored digitally); *Carpenter,* 138 S. Ct. at 2220 (holding that historical records about an individual's location "implicate[] privacy concerns far beyond those considered" in earlier cases involving data collected by more primitive technologies).

Much of this sensitive information about a person's private life can be gleaned not just from the content of a photograph, text message, or phone call, but from other information, often called metadata, that is created alongside or associated with that content. And even small amounts of these types of data can provide a striking window into a person's life. For example, telephone records can show that a person called a suicide hotline late at night near the Golden Gate Bridge by showing the numbers dialed, the time of the call, and the location of the caller. *See* EFF, *Why Metadata Matters* (March 12, 2019).[4] From that data alone, one can easily infer both the purpose of the call and the caller's likely mental state at the time; law enforcement does not need access to the contents of the phone call

[4] https://ssd.eff.org/en/module/why-metadata-matters.

to understand private details about that person's life.

Indeed, our digital communications and records reflecting our movements now generate so much data about our daily lives that law enforcement is operating in a golden age of surveillance. Peter Swire, *The Golden Age of Surveillance*, Slate (July 15, 2015).[5] And yet law enforcement manages to obtain much of this data, which reveals the "privacies of life," *Riley*, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)), without a warrant. Swire, *The Golden Age of Surveillance*.

The public has a legitimate interest in disclosure of judicial records reflecting the government's surveillance activities because, as described above, the Supreme Court has questioned whether the Fourth Amendment's pre-digital distinction between contents of communications and other information associated with it remains valid. *See Carpenter*, 138 S. Ct. at 2220; *see also* Steven M. Bellovin et al., *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 Harv. J.L. & Tech. 1 (2016) (arguing against outdated content/non-content distinction in light of the complex architecture of the Internet).

Disclosure of travel data that the FBI requested in the AWA application at

[5] https://slate.com/technology/2015/07/encryption-back-doors-arent-necessary-were-already-in-a-golden-age-of-surveillance.html.

issue here raises the same privacy concerns articulated by the Supreme Court in *Carpenter*. Just like in that case, air travel data creates "a detailed chronicle of a person's physical presence" that goes well beyond knowing a person's location at a particular time. 138 S.Ct. at 2220. However, unlike individual phone companies or ISPs, all travel data, including airline reservations and itineraries, is held by just three companies that do not appear to have any direct relationship with ordinary people. Brewster, *Global Surveillance Tool*. Sabre is the largest and oldest of those three, with data that could go back as much as fifty years. Gary Anthes, *Sidebar: Sabre Timeline*, Computerworld (May 31, 2004).[6] This means that access to the location and travel data held by the company could be especially revealing.

Given the technical and legal questions surrounding the extent to which travel data should be protected by the Fourth Amendment (thereby requiring authorities to obtain a search warrant before obtaining that information), the public has a legitimate interest in seeing the judicial records sought by Forbes Media. The records are likely to contain the court's legal analysis and legal arguments made by the government in support of its request to use the AWA to track a person's location. That would likely include the court's analysis of whether federal surveillance statutes and the Fourth Amendment were either inapplicable or satisfied. Thus the materials, including the opinion and any interpretation of the

[6] https://www.computerworld.com/article/2564361/sidebar--sabre-timeline.html.

AWA, are subject to the public's presumptive rights of access. *See Banks v. Manchester*, 128 U.S. 244, 253 (1888) ("The whole work done by the judges constitutes the authentic exposition and interpretation of the law, which, binding every citizen, is free for publication to all . . . ."); *Nash v. Lathrop*, 6 N.E. 559, 560 (Mass. 1886) ("Every citizen is presumed to know the law thus declared, and it needs no argument to show that justice requires that all should have free access to the opinions."); *see also* Appellants' Opening Brief ("AOB") at 1-3.

II. THE PUBLIC KNOWS VERY LITTLE ABOUT JUDICIAL REASONING AUTHORIZING GOVERNMENT EFFORTS TO USE THE ALL WRITS ACT TO COMPEL THIRD PARTIES TO AID SURVEILLANCE.

As this case demonstrates, the government relies upon the AWA to help it carry out traditional surveillance activities that are arguably governed by other statutory authority. But law enforcement continues to cloak its use of this legal mechanism in secrecy. Although the government appears to view the AWA as a malleable tool that authorizes surveillance and compels private parties to assist with investigations, its legal theories and activities regarding the AWA's ability to force disclosure of private digital data remain largely under seal. This ongoing secrecy violates the public's right of access to judicial records and, critically, it also frustrates public and congressional oversight of law enforcement surveillance, including whether the Executive Branch is evading legislative limits on its surveillance authority. As explained below, recent examples demonstrate that the

government often pursues novel legal theories in support of surveillance efforts while also shielding those theories from the public. Once those theories are made public, and subject to appellate review, they often prove to be incorrect or unconstitutional.

A. There Are Significant Legal Questions Concerning Whether the AWA Permits Law Enforcement to Track People's Travels.

Public access to the records Forbes Media seeks is essential because the public has right to know whether the AWA authorizes law enforcement to obtain real-time surveillance of a person. Interpreting the AWA to authorize courts to require that Sabre provide real-time tracking of an airline passenger's movements raises significant questions about congressional intent to authorize such pervasive surveillance, as well implicating the Fourth Amendment. If the courts are to interpret the AWA in this way, they should do so in the public view.

In 1977, the Supreme Court affirmed the government's use of the AWA to require a telephone company to provide technical assistance by installing a pen register on two telephone lines. *United States v. New York Telephone*, 434 U.S. 159 (1977). After *New York Telephone*, Congress passed the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2510 *et seq.*, which contains provisions that permit law enforcement to seek technical assistance orders in support of the underlying surveillance authorized by courts. *See*, *e.g.*, 18 U.S.C. § 3123(b)(2) (authorizing courts to issue technical assistance orders in support of pen

register requests). Congress also subsequently enacted the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. 103-414, 108 Stat. 4279 (1994), which "requires telecommunications carriers and manufacturers of telecommunications equipment [to] design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information"[7] while exempting providers of "information services" from those requirements. 47 U.S.C. § 1002 (b)(2). These statutes delineate the circumstances for authorizing electronic surveillance and related technical assistance with a clarity and specificity absent from the AWA.

Against this statutory backdrop, interpreting the AWA to authorize courts to require that Sabre provide real-time tracking of an airline passenger's movements raises significant questions under the Fourth Amendment and pen register statute, and implicates other concerns than those in *New York Telephone*.

The existence of an underlying arrest warrant does not allay the constitutional concerns regarding the AWA's ability to permit real-time tracking. Although courts have long issued AWA orders to authorize third-party assistance in effectuating arrest warrants, they generally do so only "where no Fourth Amendment privacy rights or other constitutional issues are implicated." *In re*

[7] *Communications Assistance for Law Enforcement Act*, Federal Communications Commission, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

Application of U.S. for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone, 849 F. Supp. 2d 526, 581 (D. Md. 2011). "The All Writs Act does not excuse the government from its burden of establishing probable cause where constitutionally protected information is requested." *Id*.[8]

The AWA application here raises these constitutional concerns. For all the reasons described above in Section I., the AWA application seeking travel data from Sabre implicates the Fourth Amendment's privacy protections under *Carpenter*. *See* 138 S.Ct. at 2220. If the disclosure demand to Sabre implicated the Fourth Amendment, then arguably the government should have obtained a search warrant before seeking the information.

Given that the judicial records Forbes Media seeks here remain under seal, neither amici nor the public know whether law enforcement obtained a search warrant for the location data sought from Sabre. But based on the unsealed AWA

[8] Court authorization of AWA orders often turn on whether the government's requests implicate the Fourth Amendment. *See United States v. X*, 601 F. Supp. 1039, 1042-43 (D. Md. 1984) (using the All Writs Act to authorize production of toll records, finding no subscriber privacy interest in them); *United States v. Doe*, 537 F. Supp. 838, 840 (E.D.N.Y. 1982) (using the All Writs Act to authorize a production of toll records as subscriber has no legitimate expectation of privacy in them); *Application of the United States of America for an Order Directing X to Provide Access to Videotapes*, No. 03-89, 2003 WL 22053105, at *2 (D. Md. Aug. 22, 2003) (authorizing access to surveillance videotapes of the public areas of an apartment complex under the All Writs Act after holding that there was "no reasonable expectation of privacy, on the part of the apartment complex tenants or their visitors, in the hallway of the apartment building").

application, it appears unlikely that it did so. Instead, the government represented in its application that courts have concluded that the AWA provides sufficient authority to compel Sabre to disclose this private data in real time on a prospective basis. *See* ER 85 (representing that the government has used the AWA to obtain "real-time" transmission of information from credit card companies and has also used it to order Sabre to assist with other arrest warrants).

Further, even if the private data sought from Sabre was not subject to the Fourth Amendment's warrant requirement under *Carpenter*, it does not appear that the government believed it needed to obtain a subpoena, court order, or other judicial process under ECPA or other statutes that protect individual privacy.

Because Congress has not enacted laws that expressly authorize either the collection of people's travel records in real time, courts should be skeptical of any government claim that the AWA can fill the gap in legal authority. *See* Jennifer X. Luo, *Decoding Pandora's Box: All Writs Act and Separation of Powers*, 56 Harv. J. on Legis. 257, 282-84. (2019) ("Luo, *Pandora's Box*"). After all, that gap may be the result of lawmakers' inability to reach consensus on whether such surveillance should be used at all. *See id*.

Given the varied ways in which law enforcement seeks to use the AWA and the potential problems with relying on the statute discussed above, the public has a legitimate interest in seeing the court's interpretation and enforcement of the

statute. Disclosure of the court's order will necessarily lead to a better understanding of when and how the government relies on the statute as part of its investigations and surveillance activities. Indeed, access may be essential for not just the public, but other courts, Congress, and other companies similarly situated to Sabre to better understand interpretations of the AWA pushed by the government in largely *ex parte*, under seal cases where it faces no adversarial process.

B. If Law Enforcement Relies on the All Writs Act to Authorize Novel Surveillance, the Court Orders and Other Judicial Records Reflecting Those Efforts Should Not Remain Under Seal.

Historically, the government's reliance on the AWA to support surveillance efforts has been quite public. In *New York Telephone*, the government did not litigate the technical assistance question under seal, and the case eventually landed in the Supreme Court. 434 U.S. at 174-78. There, the Court established a test for when and how the government could use the AWA to compel a third party to provide assistance in support of another lawful order, such as a search warrant. *Id*. at 174-76.

Federal law enforcement has apparently had success in convincing courts—in *ex parte* proceedings—that the AWA authorizes novel and controversial surveillance and law enforcement techniques. Meanwhile, court seals over these proceedings have largely kept the public in the dark about these novel legal

theories. Most notably, recent reporting has described how the government mainly uses the AWA to compel private parties' assistance in decrypting people's smartphones or other devices. *See* Luo, *Pandora's Box*, 56 Harv. J. on Legis. at 258-60. As amicus ACLU has documented, the government has sought more than sixty AWA orders compelling companies such as Apple and Google to unlock physical devices or to decrypt data. Matthew Segal, *Lessons From the Government's 63 Prior Attempts to Make Tech Companies Unlock Devices*, Slate (Mar. 31, 2016)[9] ("Segal, *Lessons*"); Luo, *Pandora's Box*, 56 Harv. J. on Legis. at 258-59. But prior to a public decision by a magistrate judge in 2015 and an FBI effort months later to unlock the iPhone of the shooter involved in the San Bernardino attack, little was known about these efforts because the government sought—and courts granted—sealing of the judicial records associated with the requests. *See In the Matter of the Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203* ("*In re San Bernardino iPhone*"), No. ED 15-0451M, 2016 WL 618401 (C.D. Cal. Feb. 16, 2016); *In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016) .

From the information that has become public, we know that the nature of the

[9] http://www.slate.com/blogs/future_tense/2016/03/31/the_government_s_63_prior_attempts_to_use_the_all_writs_act_to_make_companies.html.

government's use of the AWA to access smartphones and other devices has evolved over time. In earlier cases, the government conceded that it could not use the AWA to compel device manufacturers like Apple to decrypt data or devices. *See* Segal, *Lessons*. But in the public fight with Apple regarding access to the San Bernardino shooter's iPhone, law enforcement relied on the AWA when it sought a court order requiring Apple to help the government decrypt the phone's data by writing custom software for that phone. *Id*.

As this case shows, it appears the government views the AWA as capable of applying in a variety of circumstances, including to compel private companies to track people's travels in real time. ER 85; Brewster, *Global Surveillance Tool*. As the government further notes in the application, however, "[a]ll these AWA orders remain under seal," stymieing public understanding of courts' interpretations of the law. ER 85.

Yet there are legitimate legal questions regarding whether the AWA permits courts to order uninvolved third parties to assist law enforcement when Congress has not expressly mandated such technical assistance. *See* Luo, *Pandora's Box*, 56 Harv. J. on Legis. at 273-78. CALEA exempted information services providers such as Apple from its requirements and did not impose on private parties an obligation to decrypt "any communication encrypted by a subscriber or customer." 47 U.S.C. § 1002(b)(2)-(3). Yet this did not stop the government from attempting

to use the AWA to compel Apple to decrypt a suspect's iPhone. *In re Apple, Inc.*, 149 F.Supp.3d 341, 352-54, 359-64 (E.D.N.Y. 2016) (rejecting the government's demand because CALEA, a more specific statute than the AWA, exempts information services providers such as Apple from technical-assistance obligations).

C. The Government's Novel Interpretations of the AWA are Reminiscent of its Efforts to Push the Limits of Other Surveillance Authorities.

The government has in the past pushed for interpretations of other laws to engage in surveillance or to otherwise obtain data that did not hold up to legal scrutiny. For example, the government had for years used court orders under Section 2703(d) of the Stored Communications Act (SCA), 18 U.S.C. § 2703(d) ("D Orders"), to obtain people's location records. The government had also relied on the same law to obtain the contents of people's stored email communications. Once public, courts rejected the government's interpretations of Section 2703(d) and prohibited the government from relying on those authorities to obtain that sensitive data. *See Carpenter*, 138 S.Ct. at 2221 ("Consequently, an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records.");[10] *United States v. Warshak*, 631 F.3d 266, 288 (6th

[10] Even after *Carpenter*, law enforcement continued to try to access location information in novel ways, as at least one district court has upheld "hybrid" PRA

Cir. 2010) (holding that the government may not use the SCA "to compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause"). The public thus has a legitimate interest in learning whether the government is attempting to stretch the AWA to authorize invasive surveillance along similar lines.

Similarly, in another case involving the Lavabit encrypted email service, investigators attempted to force disclosure of encryption keys pursuant to a pen register order and an SCA seizure warrant. *See In re Under Seal*, 749 F.3d 276, 281–83, 285 (4th Cir. 2014). However, it is not clear that either the PRA or the SCA authorizes the seizure of encryption keys, and the Fourth Circuit declined to reach that issue. *See id.* at 293 (holding issue waived because not challenged below).

Law enforcement agencies have also used the PRA to seek access to data that is different than the traditional dialing and routing information the statute envisions, such as to track a device in real time. *See In re the Application of the United States for an Order*, 411 F. Supp. 2d 678 (W.D. La. 2006). The government has also tried to obtain information about changes to a particular mobile device's

---

and SCA D orders for cell-site location information. *See United States v. Evans*, No. 5:17-CR-39-FL-1, 2018 WL 7051095, at *3-4 (E.D.N.C. Dec. 20, 2018) (holding that such hybrid orders are the "functional equivalent" of a search warrant).

subscriber information, including advance notice of termination of the account or a change in number. *In re Application of the United States of America for an Order Authorizing the Installation and Use of Pen Registers and Trap and Trace Devices*, No. 18-8561, 2018 WL 6442661, at *1 (S.D. Fla. Nov. 30, 2018).

These examples show that law enforcement regularly seeks novel or uncommon court authorizations to enable new or unusual investigatory techniques that may later be found to be unlawful. Yet there is often a long delay between the initial government attempt to access private data in new ways and the public disclosure and appellate scrutiny (if any) of law enforcement's activities. *See Carpenter*, 138 S. Ct. at 2221 (holding in 2018 that law enforcement's use of a D Order in 2011 to collect historic cell-site location information was unconstitutional). The delay in securing appellate review of the government's novel and controversial legal theories is further blunted by sealing, as it means that a "huge segment of the federal docket is not subjected to the discipline of appellate review . . .." Stephen Wm. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harv. L. & Pol'y Rev. 313, 315 (2012).

The public, Congress, and appellate courts are operating at a considerable knowledge deficit when it comes to understanding how authorities use the AWA. Public disclosure will close that gap and enable oversight, debate, and, perhaps, new legislation.

III. JUDICIAL RECORDS REFLECTING LAW ENFORCEMENT'S USE OF THE AWA REMAIN UNDER SEAL, OFTEN INDEFINITELY, FRUSTRATING THE PUBLIC'S ABILITY TO LEARN ABOUT THEIR ACTIVITIES.

The public is largely in the dark regarding whether law enforcement's reliance on the AWA raises any of the concerns described above because magistrate and district court judges routinely seal all the judicial records reflecting these activities. These sealed records can account for an estimated 47 percent of magistrate judges' dockets, and they appear to remain sealed indefinitely. *See* Smith, *Gagged, Sealed & Delivered*, 6 Harv. L. & Pol'y Rev. at 317-21 (detailing results of a study of sealed cases concerning surveillance applications and orders). Yet, as Forbes Media demonstrates in its opening brief, the AWA order and application at issue here are subject to the public's presumptive rights of access under the First Amendment and common law because, among other reasons, they are analogous to injunctions requests and related orders issued by courts that have historically been public. AOB at 35-41; 50-52. Despite the public's presumptive rights of access, there is pervasive secrecy, which often includes sealing the dockets for these matters. This results in the public lacking even basic details about how frequently law enforcement requests orders under the AWA or other statutes such as the SCA and PRA. This is problematic because, without public access to dockets and orders reflecting authorities' surveillance activities, there are almost no opportunities for public oversight or intervention by Congress.

"In our common-law tradition, the exercise of judicial power is an inherently *public* act." Stephen Wm. Smith, *Kudzu in the Courthouse: Judgments Made in the Shade*, 3 Fed. Cts. L. Rev. 177, 214 (2009). Excessive sealing of AWA applications and orders, however, stifles the public's ability to learn about the judiciary's acts. "Greater transparency" of the federal courts' secret surveillance dockets "would enable meaningful oversight not only by appellate courts but also by Congress and the general public." Smith, *Gagged, Sealed & Delivered*, 6 Harv. L. & Pol'y Rev. at 331.

Disclosure of judicial records reflecting AWA applications and orders reasonably soon after the needs for secrecy are no longer justified would allow the public and lawmakers to learn basic facts about law enforcement's activities, including when and how often they seek such orders. Disclosure may also show what types of crimes authorities are investigating and whether they are using the AWA with other legal authorities, such as the SCA and PRA, or as an enabling statute on its own. For example, because of a program created by the U.S. District Court for the Western District of Washington in response to unsealing litigation, the court began publishing twice-yearly reports reflecting basic information about how frequently courts authorize law enforcement requests under the SCA and PRA. *See Pilot Program re Applications and Orders for Pen Registers and Trap and Trace Devices and re 2703(d)*, United States District Court, Western District

of Washington;[11] *see* Aaron Mackey, *Court Report Provides New Details About How Federal Law Enforcement in Seattle Obtain Private Information Without Warrants*, EFF (Feb. 24, 2020) ("Federal law enforcement in Seattle sought an average of one court order a day to disclose people's sensitive information such as calling history in the first half of 2019").[12]

IV. DISCLOSURE WOULD ALSO HELP THE PUBLIC LEARN ABOUT SABRE'S VAST DATA COLLECTION AND DISCLOSURE PRACTICES, WHICH OCCUR WITHOUT THE PUBLIC'S KNOWLEDGE OR CONSENT.

The billion-plus people whose travel details are obtained by Sabre appear to have no meaningful way to avoid the company's data collection. *See* Brewster, *Global Surveillance Tool*. Sabre is thus unlike other services, such as email and internet service providers, that users in theory can select from based on how they collect, use, and share their customers' information. Making public how courts interpret the AWA's application to Sabre is important because most people are unlikely to be aware that the company tracks their travels and readily discloses those details to law enforcement.

Users of electronic communication services benefit and can make more

[11] https://www.wawd.uscourts.gov/pilot-program-re-applications-and-orders-pen-registers-and-trap-and-trace-devices-and-re-2703d.

[12] https://www.eff.org/deeplinks/2020/02/court-report-provides-new-details-about-how-federal-law-enforcement-seattle-obtain.

informed choices about which digital tools and services they use when they have accurate information about how the government requests user information. Right now, much of the information the public knows about government requests for users' information from these services comes from companies themselves, normally in the form of transparency reports that reveal select, aggregate information that companies choose to disclose. Transparency reporting first emerged in 2010 when Google published a global report on government requests for user data and for content takedowns.[13] Now, several of the large internet companies voluntarily issue at least yearly transparency reports.[14]

But the public appears to be in an even more disadvantaged position with respect to their knowledge of Sabre's responses to law enforcement demands. Unlike the consumer services described above, Sabre acts more like a data broker of everyone's air travels. *See* Brewster, *Global Surveillance Tool*. Sabre is thus more like a credit reporting agency than a company that provides services to users

---

[13] Google, *Transparency Report*, *Global requests for user information*, https://transparencyreport.google.com/user-data/overview?hl=en.

[14] *See, e.g.*, Facebook, *Transparency, United States*, https://transparency.fb.com/data/; Microsoft, *Law Enforcement Requests Report*, https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report; AT&T, *Transparency Report*, https://about.att.com/csr/home/governance/transparency.html; Twitter, *Transparency Report, United States of America*, https://transparency.twitter.com/en/reports/countries/us.html#2020-jul-dec.

and collects data because of that relationship. *Id*.

Moreover, to amici's knowledge, Sabre does not appear to publish a transparency report showing how frequently it receives law enforcement requests for user data. And it does not appear as though many other companies that regularly receive AWA or similar orders publish transparency reports. Indeed, many companies that receive surveillance demands from law enforcement never make that information public. *See* Jennifer Valentino-Devries, *Secret F.B.I. Subpoenas Scoop Up Personal Data From Scores of Companies*, The New York Times (Sept. 20, 2019) (reporting on how government records showed that credit reporting firms and banks "generally remained mum" about receiving National Security Letters even after being informed that they could speak publicly about them).[15]

Disclosure of the judicial records at issue here is thus crucial because the public has no way to avoid Sabre's collection of their location data and has almost no information about when and how Sabre discloses their data. Court records reflecting law enforcement demands for people's data are thus likely to be the only records of when and how Sabre responds to law enforcement requests.

Public disclosure here may also encourage Sabre to challenge similar law enforcement requests in court. The Apple case provides a useful example. As

[15] https://www.nytimes.com/2019/09/20/us/data-privacy-fbi.html.

described above, the company previously complied with dozens of government demands for assistance under the AWA, even as it was making public commitments to users' privacy and developing new security features that removed Apple's ability to comply with these demands. Katie Benner and Joseph Goldstein, *Apple Wins Ruling in New York iPhone Hacking Order*, N.Y. Times (Feb. 29, 2016).[16] Apple did not publicly challenge the law enforcement practice until a magistrate judge in New York requested Apple's views on whether the government could use the AWA to seek this type of assistance and information. *Id*.; *In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by This Court*, No. 1:15-mc-01902-JO, 2015 WL 5920207 (E.D.N.Y. Oct. 9, 2015). Once prompted by the court, Apple advocated for the security concerns of its users, arguing that the government's demand under the AWA exceeded the bounds of mandatory law enforcement assistance, arguments the magistrate judge adopted to deny the request. *In re Apple, Inc.*, 149 F. Supp. 3d at 356–57.

Disclosure of court records reflecting law enforcement surveillance thus could allow the public to advocate that Sabre commit to fighting for their users' privacy. And greater public disclosure of similar court records in the future would allow the public to verify and track whether Sabre or similar companies are

[16] https://www.nytimes.com/2016/03/01/technology/apple-wins-ruling-in-new-york-iphone-hacking-order.html.

following through on their public commitments to users' privacy.

CONCLUSION

For the reasons stated above, this Court should reverse the decisions below and order the records Forbes Media seeks be unsealed.

Dated: January 10, 2022

By: /s/ *Aaron Mackey*
Aaron Mackey

Jennifer Lynch
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
amackey@eff.org

Brett Max Kaufman
AMERICAN CIVIL LIBERTIES FOUNDATION
125 Broad Street, 18th Floor, New York, NY 10004
Email: bkaufman@aclu.org
Tel.: (212) 549-2603

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES FOUNDATION
39 Drumm Street
San Francisco, CA 94103
Email: jgranick@aclu.org
Tel.: (415) 343-0758

Jacob A. Snow
ACLU FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111

Email: jsnow@aclunc.org
Tel.: (415) 621-2493

Riana Pfefferkorn
STANFORD INTERNET OBSERVATORY
616 Jane Stanford Way
Stanford, CA 94305
Email: riana@stanford.edu
Tel.: (650) 724-6814

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amici Curiae the Electronic Frontier Foundation, American Civil Liberties Union, American Civil Liberties Union Foundation of Northern California, and Riana Pfefferkorn in Support of Plaintiffs-Appellants and Reversal complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,725 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, in 14-point font in Times New Roman font.

Dated: January 10, 2022

By: */s/ Aaron Mackey*
Aaron Mackey

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on January 10, 2022.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: January 10, 2022

By: /s/ *Aaron Mackey*
Aaron Mackey

Counsel for Amici Curiae