Case Nos. 21-16233, 21-35612

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

FORBES MEDIA, LLC, ET AL.

Plaintiffs-Appellants

v.

UNITED STATES OF AMERICA

Defendant-Appellee.

Appeal from the United States District Court for the Northern District of California
No. 4:21-mc-80017-PJH (Hon. Phyllis J. Hamilton)

Appeal from United States District Court for the Western District of Washington
No. 2:21-mc-00007-RSM (Hon. Ricardo S. Martinez)

BRIEF OF *AMICUS CURIAE* RESTORE THE FOURTH IN SUPPORT OF PLAINTIFFS-APPELLANTS AND REVERSAL

Mason A. Kortz
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-495-2845
mkortz@law.harvard.edu

Counsel for *Amicus Curiae*

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus curiae* Restore the Fourth states it does not have a parent corporation, nor does any publicly held corporation own ten percent or more of its stock.

Dated: January 10, 2022

/s/ Mason A. Kortz

Mason A. Kortz

STATEMENT OF COMPLIANCE WITH RULE 29

Pursuant to Federal Rule of Appellate Procedure 29(a)(2), *amicus curiae* certifies that all parties have consented to the filing of this brief.

Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), *amicus curiae* certifies that no party's counsel authored this brief in whole or in part; no party or party's counsel contributed money that was intended to fund the preparation or submission of this brief; and no person—other than the *amicus curiae* or its counsel—contributed money that was intended to fund the preparation or submission of this brief.

Dated: January 10, 2022

/s/ Mason A. Kortz

Mason A. Kortz

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF INTEREST OF AMICUS CURIAE

Restore the Fourth, Inc. is a non-partisan non-profit dedicated to robust enforcement of the Fourth Amendment. Restore the Fourth oversees a network of local chapters whose members include lawyers, academics, advocates, and ordinary citizens. Restore the Fourth has published issue briefs on electronic surveillance techniques, including both law enforcement technologies such as IMSI-catchers and non-law enforcement technologies like smart city sensors. Accordingly, Restore the Fourth has a strong interest in transparency around government use of private actors to conduct electronic surveillance. Restore the Fourth has also filed amicus briefs in many significant Fourth Amendment cases. *See, e.g.*, Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Petitioner, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (No. 16-402); Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Plaintiff-Appellee Araceli Rodriguez, *Rodriguez v. Swartz*, 899 F.3d 719 (9th Cir. 2018) (No. 15-16410). Restore the Fourth has both the subject matter expertise and the legal knowledge to comment on the history of modern surveillance statutes and the need for public accountability.

SUMMARY OF ARGUMENT

The All Writs Act was enacted in 1789, making it one of the first statutes passed by the then-new United States legislature. In the more than two centuries since, the Act has largely been held in abeyance, used only as an extraordinary remedy in situations where Congress has not granted the authority necessary for courts to exercise their jurisdiction. This is even more true in the modern era, where courts operate under robust statutory regimes with detailed grants of—and limitations on—judicial authority. This is particularly true of modern surveillance authorizing statutes: the Wiretap Act, Stored Communications Act, and Pen Register Act all contain specific procedures for obtaining surveillance orders, as well as built-in reporting and notice requirements.

These very safeguards may have driven law enforcement agencies to use the All Writs Act to enlist private actors to conduct surveillance that the agencies could not legally perform themselves. The Court need not decide today whether such use of the All Writs Act is appropriate; the present issue is whether the public is even allowed to learn about such orders. However, this case is not just about the public's abstract, albeit important, right to know what the government is doing. Awareness is a key element of accountability. Public scrutiny encourages courts to be judicious and consistent in their decisions; public pressure can motivate Congress to act; and public transparency allows individuals and organizations to mount legal challenges

to potentially unlawful forms of surveillance. Accordingly, *amicus* respectfully urges the Court to reverse the decision below, hold that both a First Amendment and common law right of access attach to the judicial records at issue, and order the disclosure of the non-identifying portions of those records.

ARGUMENT

The All Writs Act ("AWA") is an 18th-century law that Congress enacted to fill gaps in the nascent judiciary's powers. Unlike modern surveillance statutes such as the Wiretap Act, Pen Register Act, and Stored Communications Act, the AWA does not enumerate specific procedures for courts to follow when issuing writs. This lack of procedural guidelines, combined with the AWA's role as an extraordinary form of relief, weighs heavily in favor of greater transparency around law enforcement use of AWA writs for surveillance assistance. Without such transparency, the courts, Congress, and the public will be left in the dark as to the frequency and rationale behind law enforcement agencies' use of the AWA, preventing any kind of meaningful response to, or checks on, government surveillance.

I. The history and purpose of the All Writs Act distinguish it from statutes that authorize specific forms of technical surveillance.

The portion of the AWA relevant to writs of technical assistance is brief: "The Supreme Court and all courts established by Act of Congress may 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). This language harkens back to a time when there was little statutory authority for courts to follow and many judicial powers were held over from British common law. By contrast, federal courts today operate under specific grants of authority, especially when it comes to authorizing surveillance.

A. The All Writs Act is an extraordinary and limited grant of authority, created to fill gaps in judicial power.

The AWA has its roots in English common law. Writs were used by courts as early as the Anglo-Saxon era to issue official orders. In their early days, courts endeavored to keep the number of writs to a minimum for clarity and consistency. *See* Aaron Belzer, *From Writs to Remedies: A Historical Explanation for Multiple Remedies at Common Law*, 92 Denver L. Rev. F.1, 2 (2016). By the end of the 12th century, the temptation to apply writs to accommodate a wide variety of legal circumstances led to overuse. *See id.* at 3. In response, the Provisions of Oxford 1258 prohibited the establishment of new writs without the king's permission. *Id.*

It was this limited conception of general writs that the United States imported into its nascent judicial system. *Id.* at 3. The AWA was codified into law as Sections 13 and 14 of the Judiciary Act of 1789, the very first law regarding the nature of the judiciary. *See In re Apple, Inc.*, 149 F. Supp. 3d 341 (E.D.N.Y. 2016). In her scholarship, Justice Sandra Day O'Connor called the Judiciary Act one of "'the triad of founding documents, along with the Declaration of Independence and the

Constitution itself[.]'" *Id.* at 361 (quoting Sandra Day O'Connor, *The Judiciary Act of 1789 and the American Judicial Tradition,* 59 U. Cin. L. Rev. 1, 3 (1990)). As part of such an early founding document, the AWA passed through Congress at a time when judicial powers were scantly enumerated and the judicial role was only starting to crystallize. Few statutes at that time specifically authorized judicial orders, so flexibility was paramount.

"[The Supreme Court's] early view of the scope of the all writs provision confined it to filling the interstices of federal judicial power when those gaps threatened to thwart the otherwise proper exercise of federal courts' jurisdiction." *Pennsylvania Bureau of Corr. v. U.S. Marshals Serv.*, 474 U.S. 34, 41 (1985) (collecting cases from the early 1800s). Subsequent cases upheld the notion that the All Writs Act was to be used sparingly. *See American Constr. Co. v. Jacksonville, T. & K.W.R. Co.*, 148 U.S. 372, 380 (1893) (denying writ of certiorari for interlocutory appeal under AWA, absent specific authorizing statute); *McClellan v. Carland*, 217 U.S. 268, 279 (1910) (noting that, absent statutory authorization to grant writ of certiorari, "the power to grant this writ will be sparingly used").

Since then, the AWA has undergone only minor changes that did not significantly alter the effect of the law. The most significant change came in 1948 when the AWA was codified as at 20 U.S.C/ §1651(a). *See* 62 Stat. 944 (1948), *as amended* 63 Stat. 102 (1949). The codification removed the phrase "not specifically

provided for by statute" from the original text as it appeared in the Judiciary Act. *Pennsylvania Bureau of Corr.*, 474 U.S. at 41. However, subsequent case law made clear that the Court did not understand these changes as intended to alter the effect of the law. In *Pennsylvania Bureau of Correction v. U.S. Marshals Service*, the Supreme Court assessed the legislative history and concluded that Congress "intended to leave the all writs provision substantially unchanged . . . the 1948 changes in phraseology do not mark a congressional expansion of the powers of federal courts to authorize issuance of any 'appropriate' writ." *Id.* at 42.

Today, courts can invoke the AWA only when three conditions are satisfied: (1) the writ is "in aid of" the issuing court's existing jurisdiction; (2) the writ is "necessary or appropriate" to provide such aid; and (3) its issuance is "agreeable to the usages and principles of law." *In re Apple*, 149 F. Supp. 3d at 350. The Supreme Court has read this language narrowly, holding that the Act "does not enlarge" a particular court's statutory jurisdiction and it can only be applied "in aid of" such existing jurisdiction. *Clinton v. Goldsmith*, 526 U.S. 529, 534–35 (1999). Moreover, the Act is only to be used when it is necessary, rather than simply convenient. *Pennsylvania Bureau of Corr.*, 474 U.S. at 43 ("Although that Act empowers federal courts to fashion extraordinary remedies when the need arises, it does not authorize them to issue ad hoc writs whenever compliance with statutory procedures appears inconvenient or less appropriate."). Lower courts have followed the Supreme

Court's guidance, applying the AWA only to fill gaps in statutory authority. *See, e.g.*, *Twyford v. Shoop*, 11 F.4th 518, 523 (6th Cir. 2021); *United States v. Terry*, 758 F. App'x 888, 889 (11th Cir. 2019). From its inception to modern practice, courts have recognized that the AWA must be used carefully, lest it supplant forms of judicial action specifically authorized by Congress. *Pennsylvania Bureau of Corr.*, 474 U.S. at 42–43; *see also Mongelli v. Mongelli*, 849 F. Supp. 215, 220 (S.D.N.Y. 1993) ("[T]he All Writs Act must be invoked only as a last resort—it is not a 'catch-all' statute granting jurisdiction when all else fails.").

B. By contrast, modern statutes provide detailed regulations for agencies conducting, and courts authorizing, surveillance.

The open-ended nature of the AWA distinguishes it from today's surveillance-authorizing statutes. The Wiretap Act, the Stored Communications Act, and the Pen Register Act all represent modern laws granting power judges the power to authorize electronic surveillance. While each of these Acts applies in a distinct set of circumstances, they share a common history: each was motivated by congressional concerns about surveillance overreach. These contemporary authorizing statutes are characterized by detailed frameworks—and even more detailed exceptions—for how and when particular surveillance activities may be authorized. They also contain built-in transparency provisions, including reporting and notice requirements. Most significantly, each of these Acts represents Congress's attempt, at the time of enactment, to strike "a fair balance between the

privacy expectations of American citizens and the legitimate needs of law enforcement agencies." S. Rep. 99-541, 5 (1986).

The Wiretap Act, 18 U.S.C. §§ 2510–2522, was initially enacted in 1968 as Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Pub. L. 90-351, 82 Stat. 197 (1968). It had been introduced in July 1967 "in response to congressional investigations and published studies that found extensive wiretapping had been conducted by government agencies and private individuals without the consent of the parties or legal sanction." *Title III of The Omnibus Crime Control and Safe Streets Act of 1968*, Bureau of Justice Assistance, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1284. After a year of debate and several revisions, Congress passed a version that imposed formidable requirements before one can obtain an order. *Id.* An applicant must show, among other requirements: probable cause to believe that the interception will reveal evidence of a predicate felony offense; proof that normal investigative procedures have been tried and failed, or reasonably appear to be unlikely to succeed; and proof that the surveillance will be conducted in a manner minimizing the interception of unrelated communications. *See* 18 U.S.C. §§ 2516(3)(a-b); 2518(1)(c); 2518(5). Furthermore, Congress placed strict reporting requirements on both courts and federal law enforcement regarding the use of wiretaps. *See* 18 U.S.C. § 2519.

Less than twenty years later, Congress addressed unchecked surveillance once again. The Wiretap Act, which "authoriz[ed] Government interception[] under carefully subscribed circumstances," was already "hopelessly out of date." S. Rep. 99-541, 2 (1986). With new surveillance capabilities such as "radio scanners[,] cellular telephone interception[,] tracking devices[,] pen registers[,] and electronic mail interceptions" available, Congress foresaw that, without a clear governing law, "'there is no presumption that the government will strike an appropriate balance between disclosure and confidentiality.'" H. Rep. 99-647, 18-19 (1986) (quoting Richard Posner, *Privacy in the Supreme Court*, 1979 Sup. Ct. L. Rev. 173, 176 (1979)). In response, Congress passed the Electronic Communications Privacy Act of 1986 ("ECPA"). Title I of the ECPA updated the Wiretap Act to cover electronic as well as wire and oral communications, bringing a host of new technologies under the strict authorization and reporting requirements of that Act. *See* Pub. L. 99–508, 100 Stat. 1848 (1986). Titles II and III created new statutory schemes to cover other novel forms of surveillance.

Title II of the ECPA, known as the Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"), creates a detailed system of statutory privacy rights for customers and subscribers of network service providers. The SCA was "born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from

illicit access to 'stored communications in remote computing operations and large data banks that stored e-mails.'" *In re Search Warrant No. 16-960-M-1*, 275 F. Supp. 3d 605, 609 (E.D. Pa. 2017) (quoting *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015)). The three main provisions of the SCA are § 2701, which prohibits unlawful access to stored wired and electronic communications; § 2702, which allows service providers to voluntarily disclose customer communications and records; and § 2703, which established procedures for law enforcement to compel the disclosure of stored communications. H. Marshall Jarrett et al., U.S. Dep't of Just., Off. of Legal Educ., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 115 (2009), *available at* https://www.justice.gov/file/442111/download. Section 2703 in particular reflects Congress's attempts to ensure more invasive forms of surveillance would be subject to greater procedural safeguards. *Id.* at 116 ("Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not."). To the extent that the SCA allows non-warrant court orders, it spells out in detail the legal standard and the provider's right to move to quash. *See* 18 U.S.C. § 2703(d).

Lastly, Title III of the ECPA, the Pen Register Act, 18 U.S.C. §§ 3121–3127, requires the government to obtain a court order before using a pen register (a device

that captures numbers and information about outgoing calls) or a trap and trace (a device that captures numbers and information of incoming calls) on a phone line. *Electronic Communications Privacy Act of 1986*, Bureau of Justice Assistance, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285. Like the Wiretap Act and the Stored Communications Act, the Pen Register Act sets out a legal standard: the applicant must show that the information likely to be obtained under such an order is relevant to an ongoing criminal investigation being conducted by the applicant's agency. *See* 18 U.S.C. § 3122(b)(2). The Pen Register Act also includes several transparency provisions. Law enforcement agencies must keep detailed records when they install pen register and trap and trace devices, *id.* § 3123(a)(3), and the Attorney General must report to Congress the number of pen register and trap and trace orders applied for each year, *id.* § 3126.

II. Transparency around use of the All Writs Act for surveillance is necessary to support judicial, congressional, and public accountability.

As described above, the Wiretap Act, Stored Communications Act, and Pen Register Act have the characteristics of modern surveillance-authorizing statutes: they were enacted in response to specific law enforcement practices; they set out specific procedures and legal standards for agencies and courts alike; and they provide some degree of transparency. While the aforementioned Acts are not perfect, they are a far cry from the All Writs Act. The AWA lacks both *ex ante* procedural guidelines and *ex post* disclosure requirements, making it less tailored and more

opaque than modern surveillance statutes. Given this, the First Amendment and common law rights of access are essential to protect the ability of courts, Congress, and—most importantly—the American public to shape the law.

A. Transparency keeps the courts accountable to the public and to each other.

The Ninth Circuit has recognized that the presumption of access to judicial records is "based on the need for federal courts, although independent—indeed, particularly because they are independent—to have a measure of accountability and for the public to have confidence in the administration of justice." *Ctr. for Auto Safety v. Chrysler Group, LLC*, 809 F.3d 1092, 1096 (9th Cir. 2016) (quoting *United States v. Amodeo* (*Amodeo II*), 71 F.3d 1044, 1048 (2d Cir. 1995)); *see also Valley Broad. Co. v. U.S. Dist. Court for Dist. of Nevada*, 798 F.2d 1289, 1294 (9th Cir. 1986) (recognizing the importance of "promoting the public's understanding of the judicial process and of significant public events"). Both concepts—accountability and confidence—are of heightened importance where, as here, courts are operating without the strictures of a detailed legislative scheme.

Greater judicial transparency promotes public perspectives on and criticism of the judiciary, holding courts accountable. The Supreme Court has established that "[t]he operations of the courts and the judicial conduct of judges are matters of utmost public concern." *Landmark Comm. v. Virginia*, 435 U.S. 829, 839 (1978). The public interest in promoting judicial transparency connects to long-established

public access rights, which "reflect[] the antipathy of a democratic country to the notion of 'secret law,' inaccessible to those who are governed by that law." *In re Leopold to Unseal Certain Elec. Surveillance Applications and Orders*, 964 F.3d 1121, 1127 (D.C. Cir. 2020) (internal citations omitted). Greater transparency, therefore, helps restore democratic accountability in overseeing the judicial branch. As the Second Circuit wrote in a widely-cited case on the issue,

> Federal courts exercise powers under Article III that impact upon virtually all citizens, but judges, once nominated and confirmed, serve for life unless impeached through a process that is politically and practically inconvenient to invoke. Although courts have a number of internal checks, such as appellate review by multi-judge tribunals, professional and public monitoring is an essential feature of democratic control. Monitoring both provides judges with critical views of their work and deters arbitrary judicial behavior.

U.S. v. Amodeo, 71 F.3d 1044, 1048 (2d Cir. 1995). The very perception by courts that the public can observe their activities reflects accountability at work. *Leucadia, Inc. v. Applied Extrusion Techs., Inc.*, 998 F.2d 157, 161 (3d Cir. 1993) ("As with other branches of government, the bright light cast upon the judicial process by public observation diminishes the possibilities for injustice, incompetence, perjury, and fraud."). As such, transparency both wards off potential misconduct and promotes future remedies.

Transparency also increases confidence in judicial administration by demonstrating that justice is administered fairly. Absent the ability to monitor the judicial branch, the public "could have no confidence in the conscientiousness,

reasonableness, or honesty of judicial proceedings." *Amodeo*, 71 F.3d at 1048. The reverse is also true—more transparency leads to more confidence and trust in the judicial branch. As circuit courts have widely recognized, a greater public view into the judiciary helps promote public understanding of, respect for, and belief in the fairness of, the judiciary as an institution. *See Leucadia*, 998 F.2d at 161; *Matter of Cont'l Illinois Securities Litig.*, 732 F.2d 1302, 1308 (7th Cir. 1984) (recognizing the "public's right to monitor the functioning of our courts, thereby insuring quality, honesty and respect for our legal system"); *Romero v. Drummond Co., Inc.*, 480 F.3d 1234, 1245 (11th Cir. 2007) ("The common-law right of access to judicial proceedings, an essential component of our system of justice, is instrumental in securing the integrity of the process" (internal quotations omitted)). However, greater transparency is a prerequisite to promoting these interests: "Americans cannot keep a watchful eye, either in capitols or in courthouses, if they are wearing blindfolds." *Binh Hoa Le v. Exeter Fin. Corp.*, 990 F.3d 410, 417 (5th Cir. 2021). Transparency is critical to effectuating the goals the judiciary serves. *In re Bair Hugger Forced Air Warming Devices Products Liab. Litig.*, 9 F.4th 768, 791 (8th Cir. 2021) ("Interests served by the common-law right include bolstering public confidence in the judicial system by allowing citizens to evaluate the reasonableness and fairness of judicial proceedings, allowing the public to keep a watchful eye on

the workings of public agencies, and providing a measure of accountability to the public at large . . . .").

Transparency also keeps judges informed about decisions reached by other courts. The Ninth Circuit has stated its interest in following language that promotes consistency between its decisions and those of other circuits. *Ctr. for Auto Safety*, 809 F.3d at 1102 ("We choose to follow language in our case law that makes sense and is consistent with our fellow circuits."). However, without an awareness of the contents of sealed AWA orders, courts at the district court and circuit court levels lack critical information to consider in their decision-making. Transparency is a prerequisite for consistency in courts' judicial processes and decisions, particularly when the governing statute—in this case, the AWA—grants little in the way of procedural safeguards.

B. Transparency is necessary for Congress to effectively respond to surveillance overreach.

Courts are not the only branch of government tasked with checking executive power. When courts have been unwilling or unable to contain surveillance overreach, Congress has historically responded with limitations and safeguards. However, this dynamic does not operate in a vacuum. Many existing laws, including the Wiretap Act and the ECPA, were motivated by public concern about over-surveillance, often as expressed through news reporting. Without public access to

information about modern surveillance methods, Congress will be less effective in developing meaningful legislation.

The evolution of wiretapping law is a prime example of the dynamic between the courts, Congress, and the public. By the early 1900s, media outlets were reporting on public opposition to the practice of unlimited, unsupervised wiretapping. *See* Meyer Berger, *Tapping the Wires*, The New Yorker (June 11, 1938) (describing the "uproar when people got wind of the prevalence of wiretapping," leading to investigations in 1916). But when the issue came before the Supreme Court, it held that wiretapping did not violate the Fourth Amendment, giving police the green light to continue unauthorized eavesdropping. *Olmstead v. United States*, 277 U.S. 438, 466 (1928). Six years later, Congress passed the Communications Act of 1934, which the Supreme Court read to make wiretap evidence inadmissible in federal court. *See Nardone v. United States*, 302 U.S. 379, 383 (1937) (noting that "controversy has raged with respect to the morality of the practice of wire-tapping by officers to obtain evidence"). However, federal agencies continued to use wiretaps internally, including for investigations into so-called "subversive activities." Jennifer S. Granick et. al., *Mission Creep and Wiretap Act "Super Warrants": A Cautionary Tale*, 52 Loy. L.A. L. Rev. 431, 436 (2019). This led to another round of public backlash. *Id.* at 437–39. Congress, recognizing the need to "protect . . . the privacy of wire and oral communication [and] the integrity of court

and administrative proceedings," passed the Wiretap Act. Pub. L. 90–351, 82 Stat. 197, § 801 (1968).

A similar back-and-forth occurred in the lead up to the ECPA. In 1977, the Supreme Court held that law enforcement could obtain an order under the All Writs Act compelling a telephone company to install a pen register, even though there was no legislative basis for such an action. *United States v. New York Tel. Co.*, 434 U.S. 159, 177 (1977). A few years later, Congress held extensive hearings in which academics, authors, reporters, and civil rights lawyers spoke to the dangers of a national security state. *See generally 1984: Civil Liberties and the National Security State*, Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the Comm. on the Judiciary, 98th Cong. 1 (1984). At the same time, public concern over electronic surveillance was growing. *See Electronic Communications Privacy Act*, Hearings Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice of the Comm. on the Judiciary, 99th Cong. 1–2 (1986) ("Virtually every day the press reports on the unauthorized interception of electronic communications[.]"). Once again, the combination of law enforcement overreach, judicial inaction, and public outcry led to legislative reform—this time in the form of the SCA and the Pen Register Act in 1986. *See supra* § I.B. If no one had ever known that courts were authorizing pen registers

under the AWA, it is unlikely that Congress would have held hearings, let along passed legislation.

Today, law enforcement relies on the AWA to conduct extraordinary forms of surveillance, including enlisting the aid of private actors. *See*, *e.g.*, *U.S. v. Blake*, 868 F.3d 960, 866 (11th Cir. 2017) (upholding AWA order compelling Apple to assist FBI in unlocking encrypted iPad); *Matter of U.S.*, 256 F. Supp. 3d 246, 252 (E.D.N.Y. 2017) (denying AWA order compelling provider to intercept cellphone communications); *In re Application of U.S. for an Ord. Directing X to Provide Access to Videotapes*, No. 03-89, 2003 WL 22053105, at *3 (D. Md. Aug. 22, 2003) (authorizing AWA order compelling apartment complex to produce security footage). While the full scope of these requests remains unknown, independent investigations suggest they are far from uncommon. *See* Eliza Sweren-Becker, *This Map Shows How the Apple-FBI Fight Was About Much More Than One Phone*, ACLU (March 30, 2016), https://www.aclu.org/blog/privacy-technology/internet-privacy/map-shows-how-apple-fbi-fight-was-about-much-more-one-phone (reporting on more than 70 decryption orders under the AWA between 2008 and 2016). All of this suggests that, like wiretaps in the 1960s and electronic surveillance in the 1980s, AWA technical assistance orders are ripe for reform, or at the very least public debate. However, the interplay of public pressure and congressional

concern that played out in the past cannot occur if the government is permitted to keep AWA orders like the ones at issue in this case secret.

C. Transparency allows the public to mount challenges to potentially unlawful forms of surveillance.

While federal legislation has been an important element in checking surveillance overreach, it has rarely been sufficient. When Congress has been unable or unwilling to provide adequate protection, the public has stepped in to take reform into its own hands, either in a court of law or the court of public opinion. However, for the people to object to their government's actions, they must first know that those actions are taking place. If AWA orders like the ones at issue in this case remain sealed, then systems of public accountability break down.

"Public accountability consists of two components: the explanation and justification of agencies' activities to the public; and an accompanying mechanism for public sanctions." Jennifer Shkabatur, *Transparency With(out) Accountability: Open Government in the United States*, 31 Yale L. & Pol'y Rev. 79, 82 (2012). Sanctions may take many forms, from criticism to electoral consequences. In the realm of government surveillance, lawsuits are an impactful enforcement mechanism. For example, lawsuits have been essential in filling gaps in the SCA. Much as the Wiretap Act failed to keep pace with developments in electronic communication, the SCA has failed to keep pace with cloud computing, cellular networks, and other technologies that are now commonplace. *See* Daniel J. Solove,

Reconstructing Electronic Surveillance Law, 72 Geo. Wash. L. Rev. 1264, 1292 (2004). However, individual litigants and civil society have been able to plug at least some of these holes. *See, e.g.*, *Carpenter v. United States*. 138 S. Ct. 2206, 2209 (2018) (holding that warrantless access to cell phone location data under the SCA violated the Fourth Amendment); *United States v. Warshak*, 631 F.3d 266, 285-86 (6th Cir. 2010) (holding that warrantless access to emails under the SCA violated the Fourth Amendment).

In other circumstances, sanctions have taken the form of media exposure. In 2016, the federal government obtained an AWA order compelling Apple to decrypt an iPhone in the wake of a mass shooting. *See* Eric Lichtblau and Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, New York Times (Feb. 17, 2016), https://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html. The case garnered significant public attention, bringing the little-known 1789 Act into the spotlight and fueling debate about the role of both the government and corporations in personal privacy. *See* Laura Sydell, *Can A 1789 Law Apply to an iPhone?*, NPR (Feb. 19, 2016), https://www.npr.org/sections/alltechconsidered/2016/02/19/467299024/can-a-1789-law-apply-to-an-iphone; Dan Froomkin and Jenna McLaughlin, *FBI vs. Apple Establishes a New Phase of the Crypto Wars*, The Intercept (Feb. 26 2016), https://theintercept.com/2016/02/26/fbi-vs-apple-post-crypto-wars/. Moreover, as

stated above, public attention can often be the catalyzing factor in congressional actions. *See supra* § II.B.

Whether in the courts or in the public eye, though, no response is possible without knowledge of the underlying government action. In *Carpenter* and *Warshak*, the defendants learned of the SCA orders when the government sought to admit evidence at trial. *Carpenter*, 138 S. Ct. at 2212; *Warshak*, 631 F.3d at 281. In the case of the iPhone, Apple chose to publicize the AWA order rather than to comply quietly. *See A Message to Our Customer*s, Apple (Feb. 16, 2016), https://www.apple.com/customer-letter/. Technical assistance orders like the ones at issue here are capable of evading scrutiny on both fronts. *See Blake*, 868 F.3d at 969 (noting that criminal defendants may not have standing to challenge AWA technical assistance orders); *In re Apple*, 149 F. Supp. 3d at 348 (noting that Apple had unlocked devices in at least 70 instances before objecting).

The public demand for accountability starts at transparency. As Justice Brandeis famously stated, "sunlight is said to be the best of disinfectants." Louis Brandeis, *Other People's Money and How the Bankers Use It* (1914). When information about the very fact of government action is concealed, the public's "ability to provide input, oversight, and criticism relating to that information is not simply inhibited but nullified. Nothing but the secret-keepers' good faith connects them, as agents, to their citizen-principals or to other agents in government." David

E. Pozen, *Deep Secrecy*, 62 Stan. L. Rev. 257, 279 (2010). Secrecy takes the most powerful tool for accountability—public scrutiny—away from the very people the government is meant to serve.

CONCLUSION

Both the First Amendment and common law rights of access require courts to consider the public benefits of judicial transparency. *See Press-Enter. Co. v. Superior Ct. of California for Riverside Cty.*, 478 U.S. 1, 11 (1986) (weighing benefits of public access to criminal proceedings under the First Amendment test); *Kamakana v. City & Cty. of Honolulu*, 447 F.3d 1172, 1179 (9th Cir. 2006) (noting that courts must consider the public's interests under the common law test). Here, the extraordinary nature of the All Writs Act weighs strongly in favor of disclosure. Accordingly, *amicus* respectfully urges the Court to reverse the judgment below and order disclosure of non-identifying portions of the orders at issue.

Dated: January 10, 2022

Respectfully submitted,

/s/ Mason A. Kortz

Mason Kortz
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-495-2845

mkortz@law.harvard.edu

Counsel for *Amicus Curiae*[*]

[*] *Amicus curiae* would like to thank Harvard Cyberlaw Clinic Fall 2021 students Adira Levine, Caleb O'Quinn, and Breanne Parker for their invaluable contributions to this brief.

CERTIFICATE OF COMPLIANCE

Pursuant to the Fed. R. App. P. 32(a)(7)(C), I hereby certify that:

This brief complies with the type volume limitations of Fed. R. App. P. 29(a)(5) and 32(a)(7)(b) and Ninth Circuit Rule 32-1(a) because it contains 5,116 words as calculated by the word count feature of Microsoft Word 365, exclusive of the sections exempted by Fed. R. App. P. 32(f); and

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5)(A) and (a)(6) because it uses 14-point proportionally spaced Times New Roman font.

Dated: January 10, 2022

Respectfully submitted,

/s/ Mason A. Kortz

Mason Kortz
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-495-2845
mkortz@law.harvard.edu

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing Brief of *Amicus Curiae* Restore the Fourth in Support of Plaintiffs-Appellants and Reversal 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 this case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECC system.

Dated: January 10, 2022

Respectfully submitted,

/s/ Mason A. Kortz

Mason Kortz
Cyberlaw Clinic
Harvard Law School
Wasserstein Hall, Suite 5018
1585 Massachusetts Avenue
Cambridge, MA 02138
617-495-2845

mkortz@law.harvard.edu