No. 17-2

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA,
Petitioner,

v.

MICROSOFT CORPORATION,
Respondent.

On Writ of Certiorari to the United States Court of Appeals for the Second Circuit

---

BRIEF *AMICI CURIAE* OF THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS AND XX MEDIA ORGANIZATIONS, IN SUPPORT OF RESPONDENT

Laura R. Handman
Alison Schary
Davis Wright Tremaine LLP
1919 Pennsylvania Ave. NW, Suite 800
Washington, D.C. 20006
laurahandman@dwt.com
(202) 973-4200

Bruce D. Brown
Counsel of Record
Caitlin Vogus
Selina MacLaren
The Reporters Committee for Freedom of the Press
1156 15th St. NW, Suite 1250
Washington, D.C. 20005
bbrown@rcfp.org
(202) 795-9300

(Additional counsel for amici listed in Appendix B)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

STATEMENT OF INTEREST[1]

Amici curiae are [TK] news media organizations [TK and trade organizations] that support and represent journalists and publishers who work worldwide. News media organizations and reporters rely on technology, including email and cloud-based storage services, provided by companies like Microsoft to report on issues of public interest around the world. They also routinely rely on press protections codified in U.S. law that shield newsgathering from government intrusion. By distinguishing between different types of legal process, such as subpoenas and warrants, these protections restrict prosecutorial power in meaningful ways. *Amici* urge the Court to consider how the outcome in this case might impact those press protections and encourage reciprocal demands for information by foreign governments, chilling important reporting to the detriment of an informed public.

---

[1] Pursuant to Sup. Ct. R. 37, counsel for *amici curiae* state that no party's counsel authored this brief in whole or in part; no party or party's counsel made a monetary contribution intended to fund the preparation or submission of this brief; no person other than the *amici curiae*, its members or its counsel made a monetary contribution intended to fund the preparation or submission of this brief; and letters consenting to the filing of *amicus* briefs are on file with the Clerk of the Court.

SUMMARY OF ARGUMENT

Twenty-first century journalism is a global and networked endeavor, made possible by technology. Reporters rely on technology to communicate with their sources by email, store and share newsgathering materials in cloud-based storage devices, and work collaboratively on stories from remote locations. Even before the modern newsroom migrated to the cloud, governments sought to "annex the journalistic profession as an investigative arm of government," demanding the materials journalists gathered and drafted in the course of reporting the news. *Branzburg v. Hayes*, 408 U.S. 665, 725 (1972) (Stewart, J., dissenting).

While the subscriber at issue may not be a journalist, the Court's decision in this case will necessarily impact all users of cloud-based platforms, including the journalists employed and represented by *amici*. Today, with journalists' work product necessarily in the hands of third-party service providers, technology makes the threat of that annexation all the more possible.

Amici's concern is not merely domestic. Journalists work all over the world, reporting on topics that may be of particular interest to governments, including foreign governments hostile to press rights. The United States has long been the standard-bearer for press rights by, *inter alia*, recognizing the sensitivity of reporter work product and reporter-source communications. Especially in light of the current dangerous global climate for reporters, it is important that the United States continues to model jurisdictional restraint lest

foreign nations are emboldened to target journalists through their own demands for information.

Finally, *amici* emphasize that there are meaningful distinctions between "warrants" and "subpoenas" that undergird other laws upon which members of the press rely for protection. Altering the meaning of these long-defined terms in this case will have consequences beyond the Stored Communications Act, blurring the line between "warrant" and "subpoena" to create a hybrid form of process with the worst of both worlds — expansive scope and uncertain rules.

In sum, *amici* urge the Court, when deciding this case, to consider the impact of its decision on the ability of the news media to report on stories of public interest around the world, maintaining the strong free-press protections of U.S. law while discouraging other countries with less regard for an independent press from reaching across their own borders to chill important reporting.

ARGUMENT

I. The modern digital newsroom resides in the cloud.

Members of the news media routinely store their data and communications in the cloud as they gather and report the news to the public, and they have an acute interest in safeguarding the confidentiality of their reporting materials. Accordingly, they rely on U.S. legal protections balancing law enforcement concerns with individual privacy, as well as constitutional and statutory privileges protecting their sources and work product.

A. Cloud-based services aid effective newsgathering in the digital age.

Modern communications technology is indispensable to twenty-first century newsgathering. Reporters use email and cloud-based storage services to communicate with sources and editors, conduct research, store and send video and photos, write code, build data visualizations such as infographics, draft stories, track drafts during the editing process, prepare posts for social media, interact with audiences, and other functions essential to modern newsgathering and reporting.

These rapidly evolving products are the new tools of the journalism trade, necessary for collaboration both within the newsroom and across the globe. In 2012, the Columbia Journalism Review identified cloud-based services as "everyday tools for the modern journalist." Ann Friedman, *Essential tools of*

the trade, Columbia Journalism Review (Oct. 11, 2012), https://perma.cc/QV6H-N5UD.

For example, cloud-based technology allows newsrooms to overcome distance. The managing editor for the *Hannibal Courier-Post* explained how the use of a cloud-storage service, Google Drive, helped harmonize the work of two sister publications, allowing the remote groups to adopt uniform naming conventions, review proofs and the daily online budget, share resources, and reach a larger online audience. Tim Schmitt, *Remote locations? Here's how Google Drive can bring newsrooms together*, Gatehouse Newsroom (Sep. 22, 2016), https://perma.cc/YE9G-PZAJ. Cloud-based technology "allow[ed] every member of the editorial [team] to be involved in the digital planning process." *Id.*; *see also Indonesia's biggest media company saves 28% IT investment cost through cloud transformation*, Microsoft (Nov. 16, 2016), https://perma.cc/JN8M-9P3W (explaining how a similar cloud-storage service provided by Microsoft helped one media company's journalists and editors collaborate on stories across distance).

Newsrooms increasingly store their data on platforms operated by technology companies rather than hosting their own servers, which means that much of the activity described above is routed through and stored by companies like Microsoft. *See* Ashkan Soltani (@ashk4n), Twitter (Mar. 24, 2014, 7:32 AM), https://perma.cc/AQ4T-UGVB (independently conducted research on file with *amicus* RCFP showing that nearly half of 25 news sites evaluated used Google or Microsoft to host their

email). Although these products help reporters bring the public more newsworthy information at a faster pace, they also increase journalists' reliance on third-party technology companies to maintain the privacy of their data and the confidentiality of their sources.

Technology companies "are no longer 'just platforms' — they are shaping how journalism is practiced . . ." Francesco Marconi, *When journalism meets Silicon Valley*, Associated Press (Nov. 11, 2015), https://perma.cc/EEJ4-APFB. This is especially true of the technology companies that provide email and cloud-storage services. Because newsrooms rely on these tools and will continue to do so for the foreseeable future, any changes to the legal regime governing the security of data stored with technology companies will impact journalists and news organizations.

B. Journalists store sensitive, protected reporting materials in the cloud.

A journalist's data is inevitably revelatory of core First Amendment protected activity. In many instances, effective reporting on matters of public concern depends on journalists' ability to communicate privately with sources. Accordingly, protecting confidential sources and the newsgathering process is a paramount concern for the press. Just as "[a] free press is indispensable to the workings of our democratic society," "confidential sources are essential to the workings of the press." *In re Grand Jury Subpoena, Judith Miller*, 438 F.3d 1141, 1183 (D.C. Cir. 2006) (Tatel, J., concurring) (quoting *Associated Press v. United States*, 326 U.S. 1, 28 (1945) (Frankfurter, J., concurring)).

Confidential sources have been critical to reporting on many of the major stories of public importance in the last half century, including, most famously, the Watergate scandal. *See* David Von Drehle, *FBI's No. 2 Was 'Deep Throat': Mark Felt Ends 30-Year Mystery of the Post's Watergate Source*, Wash. Post (Jun. 1, 2005), http://wapo.st/1ok8Zxe.

Indeed, as Carl Bernstein said in a FRONTLINE interview: "I know of very little reporting in the last 30 to 40 years that has been done without use of confidential sources, particularly in the national security area." FRONTLINE (PBS), News War, Feb. 13, 2007, http://to.pbs.org/124RCVI. This perspective echoed former Washington Bureau Chief and Washington correspondent of *The New York Times*, Max Frankel, who submitted a lengthy affidavit in the famous *Pentagon Papers* case defending the use of anonymous sources, stating that without the use of "secrets," "there could be no adequate diplomatic, military and political reporting of the kind our people take for granted, either abroad or in Washington and there could be no mature system of communication between the Government and the people." *See* Aff. of Max Frankel, *United States v. N.Y. Times Co.*, Case No. 71-cv-2662 (S.D.N.Y. filed Jun. 17, 1971), http://nyti.ms/2DzC4fJ.

Investigative reporting based on confidential sources is a necessary part of the fabric of an informed democratic society and fosters the civic literacy that forms the bedrock of democratic discourse. Although identifying sources is often journalistically preferable, "[a]nonymous sources are

sometimes the only key to unlocking that big story, throwing back the curtain on corruption, fulfilling that journalistic missions of watchdog on the government and informant to the citizens." Michael Farrell, *Anonymous Sources*, SPJ Ethics Committee Position Paper, https://perma.cc/5BQB-SRA3. Indeed, without confidential sources, journalists "would be relying on the official side of the story, and the official side of a story isn't always the whole side." Lana Sweeten-Shults, *Anonymous sources vital to journalism*, USA Today (Feb. 27, 2017), https://perma.cc/AV7V-Z4K8.

But a promise of confidentiality is worth little if a reporter's emails and electronic documents can be plucked from the cloud by simply compelling a third-party service provider to turn them over, without ever examining the First Amendment issues raised by such a compelled production. Content data, as sought here, reveals the actual communications between a journalist and a source. Even a journalist's metadata can reveal the identity of a source, when and where a source and a journalist communicated, the length of their phone calls, and how frequently they are in contact. It is therefore essential that technology companies safeguard journalist data to protect the identities of confidential sources.

Even the threat of government surveillance discourages sources from speaking to reporters in the first place. In 2013, for example, the Associated Press learned that the Justice Department had seized records from twenty AP telephone lines used by more than 100 AP reporters and editors. *See*

Mark Sherman, *Gov't Obtains Wide AP Phone Records in Probe*, Associated Press (May 13, 2013), https://perma.cc/2P8J-RTPT. AP President and CEO Gary Pruitt discussed the impact of the surveillance during a speech at the National Press Club: "In some cases, government employees that we once checked in with regularly will no longer speak to us by phone and some are reluctant to meet in person." Lindy Royce-Bartlett, *Leak Probe Has Chilled Sources*, AP Exec Says, CNN (Jun. 19, 2013), https://perma.cc/VU8T-6HUP.

As this Court has recognized, a necessary corollary of the First Amendment right to publish news is a right to gather it: "[W]ithout some protection for seeking out the news, freedom of the press could be eviscerated." *Branzburg v. Hayes*, 408 U.S. 665, 681 (1972). Indeed, the public's knowledge and understanding of the functioning of government today is owed to confidential communications and confidential newsgathering methods.

II. Expanding the U.S. government's ability to reach electronic records stored outside its borders sets a dangerous international example that foreign governments hostile toward journalists may exploit.

As organizations with reporting operations around the globe, *amici* are concerned not only about this case's potential impact on press protections within the U.S., but also the possibility that it will introduce an international norm that would make journalists more vulnerable to global attacks on press freedom. Journalists already face unprecedented threats in other nations, and it is

important that the United States continue to lead by example in supporting a free press. Broadening the government's ability to reach data stored overseas may embolden other nations to target journalists operating in those countries whose data is stored outside their borders, including journalists working for U.S. news outlets.

According to a Freedom of the Press report by Freedom House, press freedom is in decline globally. *See* Freedom of the Press 2017, Press Freedom's Dark Horizon, https://perma.cc/RW3D-8X9T. The United States has long stood as a bulwark against threats to free expression and a standard-bearer of press freedom. The United States champions press rights by publicly shaming nations that attack the press,[2] playing a role in the release of reporters imprisoned abroad,[3] funding independent media,[4]

---

[2] *See* Statement on World Press Freedom Day, The American Presidency Project (May 1, 2008), https://perma.cc/J6FV-BD9E (former President George W. Bush naming countries that harass and persecute journalists).

[3] *See* Jo Biddle, *AP, Freed Vietnam dissident heads to US*, Yahoo News (Oct. 24, 2014), https://yhoo.it/2Dw3hQB (reporting that Vietnam freed one of its most prominent bloggers from custody after former President Barack Obama raised the case); *Ethiopia: Free All Jailed Bloggers and Journalists Before Obama Visit*, Amnesty International (Jul. 9, 2015), http://bit.ly/2DzYKg6 (discussing the Ethiopian government's release of four journalists and two bloggers ahead of a visit by former President Obama).

[4] *See* Reuters, *U.S. launches media fund for Hungary to aid press freedom* (Nov. 13, 2017), https://perma.cc/EJ5R-UL44 (reporting that the State Department announced a

and passing legislation that secures journalist data,[5] among other activities. Just in December 2017, the Senate unanimously passed a resolution "recognizing the pervasive threats to freedom of the press around the world," and "call[ing] on governments to investigate and resolve cases of violence against journalists." *See* Press Release: Rubio, Casey, Wyden Press Freedom Resolution Passes Senate Unanimously (Dec. 20, 2017), https://perma.cc/AJ5G-D9NS.

These actions matter. In August, for example, the State Department issued a statement urging the government of Azerbaijan to immediately release the editor-in-chief of the country's "only remaining independent media outlet." Press Statement: Statement on the Assault on Media Freedom in Azerbaijan, U.S. Department of State (Aug. 26, 2017), https://perma.cc/CDD8-43WQ. Weeks later, he was released. *See* Statement by the Spokesperson on the release of Mehman Aliyev, Council of Europe (Sept. 11, 2017), https://perma.cc/BJD7-3NEN.

Just as the United States leads by positive example, any erosion of press freedom domestically could send the signal that other nations can get away with even harsher abuse of journalists. "[W]hen it

---

fund for rural media in Hungary to train journalists in response to growing pressure and intimidation).

[5] *See* Privacy Protection Act of 1980 Statement on Signing S. 1790 Into Law (Oct. 14, 1980), https://perma.cc/UN3U-5NNE (former President Jimmy Carter discussing the importance of safeguards for the free press and the administration's commitment to "revers[ing] the historic growth in collection of personal data by the Government."

comes to press freedoms, norms are just as important as laws." Joel Simon, *The world looks to America to defend press freedom*, CNN (Nov. 15, 2017), https://perma.cc/PFQ8-QC8A. If the United States obtains overseas data without going through established international processes such as Mutual Legal Assistance Treaties ("MLATs"), other countries may also forego those processes.

Such a result will inescapably increase the pressure on technology companies like Microsoft to turn over U.S.-stored user data to other countries. To some extent, that's already happening: Lawyers for Microsoft pointed out to the district court that Chinese authorities raided four Microsoft locations, took servers from Microsoft's offices, and "demanded a password to seek e-mail information in the United States." *See* Joint App'x at 131; *see also* Resp. Br. at 58 n. 8 (noting that as the current case was pending, Brazil tried to force Microsoft to produce data stored in the United States). Other companies have faced similar demands. *See, e.g.,* Vinod Sreeharsha, *WhatsApp Is Briefly Shut Down in Brazil for a Third Time*, N.Y. Times (Jul. 19, 2016), https://nyti.ms/2kgZj3T (noting that Brazil repeatedly shut down WhatsApp and arrested a Facebook executive for not cooperating in a criminal investigation by turning over information from WhatsApp); Verne Kopytoff, *Are Google, Yahoo and Microsoft Living Up to Their Promises in China?* Time (Jan. 8, 2014), https://perma.cc/AS9U-AGT6 (noting that Yahoo turned over data to Chinese authorities that led to the arrest and imprisonment of dissents); Amar Toor, *BlackBerry won't be leaving Pakistan after all*, The Verge (Jan. 4, 2016),

https://perma.cc/A53Y-GB6B (noting that Pakistan demanded backdoor access to user data from BlackBerry).

Companies like Microsoft rely on sovereignty principles to resist foreign government demands for data. *See, e.g.,* Joint App'x at 131. Broadening the ability of the U.S. government to access emails located outside its borders would undercut this reasoning. If a U.S. court can compel a service provider to search and seize emails located anywhere in the world — without notice to the subscriber or the sovereign nation where the emails and subscriber are located — other governments could demand the same response from those service providers' subsidiaries in their own countries. In addition to seeking records from email and cloud providers, government authorities may raid local news bureaus seeking access to the emails of reporters based in the United States.

These are not academic concerns. Journalists already face very real threats from foreign governments. Due to the press's institutional role as a check on government authority, both domestically and abroad, journalists are frequent targets of state-sanctioned suppression attempts and surveillance. Foreign governments surveil and harass the press by, *inter alia*, sponsoring hacking attempts on U.S. and foreign news media.[6] Indeed, two Google

[6] *See, e.g.,* Daniel Lippman, *State-sponsored hackers targeting prominent journalists, Google warns*, Politico (Feb. 10, 2017), https://perma.cc/3SGX-ZHG3 (reporting that Google warned several journalists of attempts by state-sponsored hackers to steal their passwords and

security engineers found in 2014 that "[t]wenty-one of the world's top-25 news organizations have been the target of likely state-sponsored hacking attacks." Jeremy Wagstaff, *Journalists, media under attack from hackers: Google researchers*, Reuters (Mar. 28, 2014), http://reut.rs/1l9SpbW.

Foreign governments monitor, intimidate, and retaliate against the press in other ways as well. For example, spyware sold to the Mexican government was used to target two of Mexico's most influential journalists who were reporting on government corruption, along with the son of one of the journalists. *See* Azam Ahmed and Nicole Perlroth, *Using Texts as Lures, Government spyware Targets Mexican Journalists and Their Families*, N.Y. Times (Jun. 19, 2017), https://nyti.ms/2sGmhJ0. And in

---

break into their inboxes); Raphael Satter, Jeff Donn, and Nataliya Vasilyeva, *Russian hackers hunted journalists in years-long campaign*, Associated Press (Dec. 22, 2017), https://perma.cc/D4EA-N244 (reporting that U.S.-based journalists were targeted by hackers suspected of association with the Russian government, and noting that journalists were the third-largest group on a hacking "hit list")**;** Chris Brummit, *Vietnam's 'cyber troops' take fight to U.S., France*, Associated Press (Jan. 20, 2014), http://bit.ly/1uVl4mR (reporting that an Associated Press reporter based in Hanoi was targeted by hackers associated with the Vietnamese government); Nicole Perloth, *Hackers in China Attacked the Times for Last Four Months*, N.Y. Times (Jan. 30, 2013), http://nyti.ms/1pVnfev (reporting that Chinese hackers targeted email accounts of *New York Times* reporters for months after the newspaper published an investigative report about the secret fortune accumulated by an outgoing Chinese leader)**.**

February 2017, it was revealed that Germany had been spying on foreign journalists since 1999. *See* Alison Smale, *Germany's Intelligence Service Spied on Journalists, Report Says*, N.Y. Times (Feb. 25, 2017), https://nyti.ms/2lH5SQG.

Amici recognize that law enforcement investigations must keep pace with the digital age, and electronic surveillance may be a necessary part of those investigations. The example of the United States seizing electronic records stored outside its borders will have the ripple effect of emboldening foreign countries to target journalists. *Amici* believe these potential unintended consequences should inform the case at hand.

III. There is a meaningful distinction between warrants and subpoenas that has long been central to U.S. press protections.

The U.S. Court of Appeals for the Second Circuit observed that interpreting the SCA to prohibit application of warrants to data stored in foreign countries not only complied with the presumption against extraterritoriality, it also avoided "unintended clashes between our laws and those of other nations . . ." *Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 829 F.3d 197, 210 (2d Cir. 2016) ("*Matter of Warrant*") (quoting *EEOC v. Arabian Am. Oil Co.*, 499 U.S. 244, 248 (1991)). The Second Circuit's decision had another benefit: It avoided unintended clashes with domestic laws and procedures designed to protect the press by recognizing the meaningful distinction between warrants and subpoenas. The delineation between a

warrant and a subpoena is not only central to this case; it is also a critical to established press protections.

"[W]hen Congress employs a term of art, it presumably knows and adopts the cluster of ideas that were attached" to that term." *Id.* at 212 (quoting *F.A.A. v. Cooper*, 132 S. Ct. 1441, 1449 (2012)) (internal quotation marks and citations omitted). The term "warrant" carries with it a defined "cluster of ideas" — which include the understanding that it cannot be enforced extraterritorially. *See id.* ("[A] warrant protects privacy in a distinctly territorial way."). *See also* Microsoft Br. at [TK]. Nevertheless, Petitioner suggests that an SCA search warrant can be treated like a subpoena during its execution. *See* Pet'r Br. at 36 (stating that "[t]he execution of a[n SCA search warrant] thus functions like the execution of a subpoena"); *see also* Pet. App. 84a (magistrate judge below claiming that although an SCA search warrant is "obtained" like a "conventional warrant," "it is executed like a subpoena").

An entire regime of statutes and regulations exists in the U.S. guarding the media against overreaching government intrusion into newsgathering activities. The protections provided by this regime often depend on whether documents or other materials are sought from the press by warrant or by subpoena. By suggesting that an SCA warrant can be treated like a subpoena hybrid rather than a conventional search warrant, Petitioner muddles these long-defined terms and introduces

needless uncertainty about the protections that U.S. law affords the press.

For example, Congress recognized the importance of the subpoena-warrant distinction in enacting the Privacy Protection Act ("PPA"), 42 U.S.C. § 2000aa, which makes it unlawful for a government officer "to *search for or seize* any work product materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication." 42 U.S.C. § 2000aa(a) (emphasis added).

The PPA stemmed from *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), in which police executed a search warrant on the *Stanford Daily's* newsroom for unpublished photographs and the newspaper sued the police department for First and Fourth Amendment violations. *See* S. Rep. No. 96- 874, at 4 (1980), reprinted in 1980 U.S.C.C.A.N. 3950, 3950 (1980). In a 5-3 opinion, Justice White, writing for the majority, stated that "[w]here the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with scrupulous exactitude." *Zurcher*, 436 U.S. at 564 (internal quotations and citation omitted). The Court ultimately held that the search at issue was constitutional, leading to public outcry and the passage of the PPA.

The PPA protects newsgathering materials by banning searches where the materials sought are "work product" materials, and enacting a "subpoena-

first" rule where the government seeks "documentary materials."[7] 42 U.S.C. § 2000aa; *see also* S. Rep. No. 96-874, at 9, 1980 U.S.C.C.A.N. at 3956 ("When the materials sought consist of work product, a general no-search rule applies. When the materials sought constitute documentary materials other than work product, a subpoena-first rule is generally applicable.") In narrow circumstances where certain materials cannot be obtained by subpoena and delay would "threaten the interests of justice," the government may proceed by warrant provided that it provides the news organization notice and an opportunity to contest the seizure in court. 42 U.S.C. § 2000aa(b)(4)(c).[8]

The PPA's mechanics thus clearly differentiate between warrants and subpoenas — prohibiting search and seizure of work product and newsgathering materials by warrant, except in rare

---

[7] The statute defines "work product" materials to include materials that are "prepared, produced, authored, or created" in anticipation of dissemination to the public and which reflect the preparing party's "mental impressions, conclusions, opinions, or theories." 42 U.S.C. § 2000aa-7(b). "Documentary materials" include "materials upon which information is recorded" — such as photographs, video, audio recordings, and printed materials — that are gathered in anticipation of publication, but which are not created in anticipation of publication and do not reflect the author's mental impressions. 42 U.S.C. § 2000aa-7(a).

[8] The PPA also contains a narrow "suspect" exception that allows the government to proceed by warrant if there is probable cause to believe the person possessing the materials committed a crime and the materials relate to that crime.

instances, and requiring a "subpoena-first" approach for documentary materials. 42 U.S.C. § 2000aa(a), (b)(4). Treating a warrant like a subpoena in this case, as the government urges, would introduce uncertainty into this differentiation. One question, among others, would be how the PPA would apply to such a warrant-subpoena hybrid, or if the government would take the position that it would not apply at all.

In the past, the government has demonstrated that it considers SCA warrants to trigger the PPA's restrictions. In 2010, the government was investigating an alleged unauthorized disclosure of classified information about North Korea to Fox News journalist James Rosen. *See* Ann E. Marimow, A Rare Peek into a Justice Department Leak Probe, Washington Post (May 19, 2013), http://wapo.st/N1Qzh6. In support of an application for a search warrant to search Rosen's email, the government submitted an affidavit invoking *both* the SCA and the PPA. *See* Affidavit of Reginald B. Reyes in Support of Application for Search Warrant, ECF No. 20-1, *Application for Search Warrant for E-Mail Account [REDACTED]@gmail.com Maintained on Computer Servers Operated by Google, Inc.*, No. 10 Mag. 291 (D.D.C. Nov. 7, 2011), ¶ 3. The government addressed the PPA's general prohibition against warrant-based searches and seizures of newsrooms by alleging that the PPA's narrow "suspect" exception applied because Rosen was suspected of violating the Espionage Act as an "aider and abettor and/or co-conspirator." *Id.* ¶¶ 5, 8. Rosen's case demonstrates that, in the past, the government has treated SCA warrants like

conventional warrants, subject to the PPA's protections. *See* Michael Isikoff, *DOJ confirms Holder OK'd search warrant for Fox News reporter's emails*, NBC News (May 23, 2013), https://perma.cc/7P5L-2EBM (reporting that the government stated that the warrant was intended to comply with the PPA).

Other examples illustrate that the government understands that different SCA tools — *i.e.*, court orders, warrants, or subpoenas — are distinct, with different scopes and applications. For example, in 2012 and 2013, the government was investigating the alleged leak of information about a foiled bomb plot in Yemen by a former FBI agent to the Associated Press. As part of its investigation, the government sought both a court order issued pursuant to Section 2703(d) of the SCA (a "Section 2703(d) order") and a subpoena issued pursuant to SCA requirements to obtain different types of records of the news media.

According to judicial records that the Reporters Committee successfully petitioned to have unsealed, the government sought metadata about a reporter's emails through a Section 2703(d) order, though the order was never executed. *See* Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d), *In re Application of the United States of American for an Order Pursuant to 18 U.S.C. § 2703(d)*, Case No. 13-mc-460, ECF No. 1 ¶ 31 (D.D.C. May 7, 2013) (showing that the target email account was used by a reporter); *id.* at ECF No. 2 (D.D.C. May 7, 2013) (court order showing in Attachment A that the government sought metadata records); *id.* at

ECF No. 12 (D.D.C. May 20, 2013) (moving to vacate the order). In addition, the government also secretly obtained two months' worth of telephone records for Associated Press reporters using a subpoena. *See* Sari Horwitz, *Under sweeping subpoenas, Justice Department obtained AP phone records in leak investigation*, Wash. Post (May 13, 2013), http://wapo.st/2BZDeDq.[9]

Thus, by employing search warrants, Section 2703(d) orders, and subpoenas issued pursuant to the SCA to obtain different types of records in the Rosen and AP examples, the government showed that its policies and procedures recognize distinctions between different SCA tools, including the distinctions between warrants and subpoenas. The government's suggestion that the Court treat an SCA warrant like a subpoena or subpoena-warrant "hybrid" would introduce needless uncertainty about these long-defined and critically important terms.

These distinctions between different types of legal process are a restraint on government power and therefore critical to the protections provided to the

---

[9] The government has also recognized the distinction between subpoenas and warrants in the Justice Department's internal policies on protections for the news media from legal demands from prosecutors. *See* 28 C.F.R. § 50.10. That policy turns on distinctions between "subpoenas" — which are grouped with civil investigative demands, pen register orders under 18 U.S.C. § 3123, and court orders issued pursuant to Section 2703(d) of the SCA (*see* 28 C.F.R. § 50.10(b)(2)(i)) — and "warrants," which include SCA warrants, *see* 28 C.F.R. § 50.10(b)(2)(ii).

news media. To hold that a "warrant" is not always a "warrant" would, in effect, rewrite the SCA and threaten to erode along with it other legal constraints that have protected the press from government intrusion.

CONCLUSION

For the foregoing reasons, *amici* respectfully request that this Court consider the impact on press protections in resolving the question presented.

Respectfully submitted,

Bruce D. Brown
Counsel of Record
Caitlin Vogus
Selina MacLaren
The Reporters Committee for
Freedom of the Press
1156 15th St. NW, Suite 1250
Washington, D.C. 20005
bbrown@rcfp.org
(703) 795-9300

Month XX, XXXX

APPENDIX A

Descriptions of *amici*:

TK

APPENDIX B

Additional *amici* counsel:

TK