No. 19-16066

IN THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

CAROLYN JEWEL, TASH HEPTING, ERIK KNUTZEN, YOUNG BOON HICKS (as Executrix of The Estate of Gregory Hicks), and JOICE WALTON,

Plaintiffs-Appellants,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants-Appellees.

On Appeal from the United States District Court for the Northern District of California, No. 08-CV-04373-JSW

BRIEF OF AMICUS CURIAE THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS IN SUPPORT OF PLAINTIFFS-APPELLANTS URGING REVERSAL

Bruce D. Brown, Esq.
Counsel of Record
Katie Townsend, Esq.
Gabriel Rottman, Esq.
Linda Moon, Esq.
THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1020
Washington, D.C. 20005
Telephone: (202) 795-9300
Facsimile: (202) 795-9310
bbrown@rcfp.org

CORPORATE DISCLOSURE STATEMENT

The Reporters Committee for Freedom of the Press is an unincorporated association of reporters and editors with no parent corporation and no stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Other Authorities

STATEMENT OF IDENTITY AND INTEREST OF AMICUS CURIAE

Amicus Curiae the Reporters Committee for Freedom of the Press is an unincorporated nonprofit association. The Reporters Committee was founded by leading journalists and media lawyers in 1970 when the nation's news media faced an unprecedented wave of government subpoenas forcing reporters to name confidential sources. Today, its attorneys provide *pro bono* legal representation, *amicus curiae* support, and other legal resources to protect First Amendment freedoms and the newsgathering rights of journalists.

The Reporters Committee files this brief in support of Plaintiffs-Appellants Carolyn Jewel, Tash Hepting, Erik Knutzen, Young Boon Hicks (as executrix of the estate of Gregory Hicks), and Joice Walton (collectively, "Appellants"). Journalists rely on confidential relationships and secured communications with sources to investigate and report on important issues of public interest. The mass surveillance programs at issue in this case could threaten those relationships and the integrity of the newsgathering process. The Reporters Committee writes to highlight the importance of confidentiality and secured communications in newsgathering activities and how mass surveillance can have a chilling effect on reporter-source relationships.

SOURCE OF AUTHORITY TO FILE

Plaintiffs-Appellants and Defendants-Appellees consent to the filing of this *amicus* brief. *See* Fed. R. App. P. 29(a)(2).

FED. R. APP. P. 29(a)(4)(E) STATEMENT

Amicus declares that:

1. no party's counsel authored the brief in whole or in part;
2. no party or party's counsel contributed money intended to fund preparing or submitting the brief; and
3. no person, other than *amicus*, their members or their counsel, contributed money intended to fund preparing or submitting the brief.

INTRODUCTION AND SUMMARY OF ARGUMENT

The government's mass collection of communications content and records has a particular and substantial impact on the integrity of the newsgathering process and thus on the First Amendment and freedom of the press. Journalists often rely on sources for information about sensitive and important issues, and many sources require confidentiality before coming forward because they reasonably fear retribution if their identities are revealed, including the threat of criminal prosecution, loss of employment, and even risk to their lives. *See Introduction to the Reporter's Privilege Compendium*, The Reporters Comm. for Freedom of the Press, https://www.rcfp.org/introduction-to-the-reporters-privilege-compendium/ (last visited Sept. 6, 2019). Thus, when the threat of surveillance reaches these sources, there is a real chilling effect on quality reporting and the flow of information to the public. *See* Privacy and Civil Liberties Oversight Bd., *Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* 164 (Jan. 23, 2014), http://bit.ly/1d01fII (finding that the NSA surveillance programs deter confidential sources from speaking to journalists and stating that "[a]lthough we cannot quantify the full extent of the chilling effect, we believe that these results – among them greater hindrances to political activism and a less robust press – are real and will be detrimental to the nation").

Amicus writes to underscore the corrosive effect that dragnet surveillance has on confidential reporter-source relationships and the ability of the news media to report on matters of public interest. *Amicus* does so by discussing historical and recent examples in which journalists have relied on confidential sources to break news stories of national importance. Such examples are discussed in the context of widely recognized legal protections for reporters' sources and source materials. *Amicus* also presents them in the context of recent developments in "leak" prosecutions, which have heightened concerns that dragnet surveillance could compromise confidential reporter-source relationships through the incidental or accidental collection of communications content or records revealing the identity of a source. It is crucial for this Court to vindicate the rights of the press and the public in this case, particularly in light of the Justice Department's internal policies limiting when and how the department may investigate the press.

For these reasons, *amicus* urges the Court to reverse and remand the district court's order dated April 25, 2019.

ARGUMENT

I. The integrity of a confidential reporter-source relationship is critical to producing quality journalism, and mass surveillance compromises that relationship to the detriment of the public interest.

A. Legal protections against compelled disclosure of confidential sources recognize the importance of a confidential reporter-source relationship in the newsgathering process and in the free flow of information.

A journalist's ability to foster and maintain confidential relationships with sources is essential to effective reporting. *See Zerilli v. Smith*, 656 F.2d 705, 711 (D.C. Cir. 1981) ("[J]ournalists frequently depend on informants to gather news, and confidentiality is often essential to establishing a relationship with an informant."); *see also Introduction to the Reporter's Privilege Compendium*, The Reporters Comm. for Freedom of the Press, *supra.* When the government is permitted to indiscriminately seize journalistic records that disclose confidential sources or is able to do so without an appropriate showing of individualized suspicion of wrongdoing, journalists may become unwilling investigators for law enforcement[1] and sources are deterred from disclosing sensitive and newsworthy

[1] This Court has recognized the dangers associated with using journalists as unwilling arms of law enforcement by protecting even non-confidential journalistic work product. *See, e.g.*, *Shoen v. Shoen*, 5 F.3d 1289, 1294–95 (9th Cir. 1992) (extending a qualified reporter's privilege to non-confidential information, recognizing "the disadvantage of a journalist appearing to be an investigative arm of the judicial system or a research tool of government or of a private party" (quoting *United States v. La Rouche Campaign*, 841 F.2d 1176, 1182 (1st Cir. 1998))).

information. *See, e.g.*, Michael Barbaro, *Cracking Down on Leaks*, N.Y. Times: The Daily (June 18, 2018), https://perma.cc/7ZP5-C2BL (interview with Pulitzer Prize-winning journalist Matt Apuzzo at the New York Times, who explained that after it became public that the government had seized his records, sources advised him they could no longer talk to him). For example, when the Justice Department's seizure of the records of 30 Associated Press telephone lines used by more than 100 reporters came to light, AP President and CEO Gary Pruitt stated, "Some of our longtime trusted sources have become nervous and anxious about talking to us, even on stories that aren't about national security," and that the chilling effect was not limited to the AP. Jeff Zalesin, *AP Chief Points to Chilling Effect After Justice Investigation*, The Reporters Comm. for Freedom of the Press (June 19, 2013), https://www.rcfp.org/ap-chief-points-chilling-effect-after-justice-investigation/; *see also* Lindy Royce-Bartlett, *Leak Probe Has Chilled Sources, AP Exec Says,* CNN (June 19, 2013), https://perma.cc/K7VR-M5NB. The Associated Press eventually received notice of the subpoenas but only after the fact, and it was unable to challenge the subpoenas before the records were seized because the Justice Department delayed notifying it of the seizure.

When sources stop talking to media organizations because they fear that their identities cannot be protected, the public loses out on valuable information. Numerous courts have recognized that discouraging confidential sources from

speaking to the press stifles the vital flow of information to the public and thus undermines the electorate's ability to make informed political, social, and economic decisions and to hold elected officials and others accountable. *See, e.g.*, *Zerilli*, 656 F.2d at 711 (explaining that protection of reporters' confidential sources serves the health of a democracy by ensuring that citizens have access to information needed to make informed choices); *Ashcraft v. Conoco, Inc*., 218 F.3d 282, 287 (4th Cir. 2000) ("If reporters were routinely required to divulge the identities of their sources, the free flow of newsworthy information would be restrained and the public's understanding of important issues and events would be hampered in ways inconsistent with a healthy republic."); *see also* Alexander M. Bickel, *The Morality of Consent* 84 (1975) ("Forcing reporters to divulge such confidences would dam the flow to the press, and through it to the people, of the most valuable sort of information: not the press release, not the handout, but the firsthand story based on the candid talk of a primary news source.").

Indeed, many history-altering news stories on government (and private sector) activities would not have been possible without confidential communications between journalists and sources. One of the most famous examples is the reporting of the Washington Post's Carl Bernstein and Bob Woodward on the involvement of the Nixon administration in the Watergate break-in and subsequent cover-up. Bernstein recalled, "Almost all of the articles I co-

authored with Mr. Woodward on Watergate could not have been reported or published without the assistance of our confidential sources and without the ability to grant them anonymity, including the individual known as Deep Throat." David Kravets, *Reporters Challenge Bonds' Leak Subpoena,* Associated Press (May 31, 2006), https://perma.cc/2JS6-5N7C. Woodward often relied on a system of coded signals to set up in-person meetings with Deep Throat because the FBI official grew increasingly nervous about talking on the phone, even to set up meetings. *See* Carl Bernstein & Bob Woodward, *All the President's Men* 71 (1974); Andrew Buncombe, *How Woodward met Deep Throat*, Independent (June 3, 2005), https://perma.cc/9V7T-NZ4X.

Other major stories have similarly relied on confidential sources. The New York Times, using information provided by confidential sources, broke the story that, long before the scope of the current surveillance programs came to light, the NSA had an illegal wiretapping program that monitored phone calls and e-mail messages involving individuals suspected of involvement in terrorist activities without court review, let alone a warrant. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times (Dec. 16, 2006), https://perma.cc/UU4J-YE9U.

The Times also used confidential sources to report on the harsh "enhanced" interrogations to which terrorism suspects in U.S. custody overseas were subjected,

see David Johnston and James Risen, *Secret U.S. Endorsement of Severe Interrogations,* N.Y. Times (Oct. 4, 2007), https://perma.cc/Z922-C84R; and the U.S. government's use of drones to kill suspects, including an American citizen, *see* Scott Shane, *U.S. Approves Targeted Killing of American Cleric,* N.Y. Times (Apr. 6, 2010), https://perma.cc/KG6M-U52H. The Washington Post also relied on confidential government sources, among others, to report on the Central Intelligence Agency's use of "black sites," a network of secret prisons for terrorism suspects. *See* Dana Priest, *CIA Holds Terror Suspects in Secret Prisons,* Wash. Post (Nov. 2, 2005), https://perma.cc/ZV9V-7ZED.

Additionally, and importantly, confidential sources have been instrumental in investigative journalism into private sector wrongdoing. In a notable recent example, a consortium of investigative journalists around the world reported on the "Panama Papers," a leaked cache of data about offshore financial havens, which had been transmitted securely and anonymously to the consortium. *See* Frederik Obermaier et al., *About the Panama Papers*, Süddeutsche Zeitung, https://perma.cc/9NW2-Y2KZ (describing the nearly 50-years' worth of data illustrating fraud, money laundering, tax evasion, and evasion of international sanctions under the shelter of Panamanian corporate service provider Mossack Fonseca). This year, the International Consortium of Investigative Journalists, the hub of this transnational reporting team, announced that the global tally of fines and back-

taxes resulting from the Panama Papers reporting has totaled over one billion dollars. *See* Douglas Dalby & Amy Wilson-Chapman, *Panama Papers Helps Recover More Than $1.2 Billion Around the World*, Int'l Consortium of Investigative Journalists (Apr. 3, 2019), https://perma.cc/5XY5-AMKM.

These stories depend on the ability of journalists to assure their sources confidentiality and anonymity. Reflecting the vital role that confidential sources play in informing the public, a national consensus has emerged over the past fifty years that reporters should be legally protected from having to divulge their sources. Every state in the United States except two—Hawaii and Wyoming—recognizes legal protections for a journalist's confidential sources, providing a critical safeguard to the newsgathering process. *Reporters Privilege Compendium Map*, The Reporters Comm. for Freedom of the Press, https://www.rcfp.org/reporters-privilege/ (last visited Sept. 9, 2019). Most are statutory "shield" laws, but some are judicially recognized privileges grounded in First Amendment principles. *See id.*; *see also* Brett Spain, *Reporters Privilege Compendium: Virginia*, Part II.C, The Reporters Comm. for Freedom of the Press, https://www.rcfp.org/privilege-compendium/virginia/#c-federal-constitutional-provision (last visited Sept. 9, 2019) (explaining that the Virginia Supreme Court recognized a privilege under the First Amendment in *Brown v. Commonwealth*, 204 S.E.2d 429 (Va. 1974)).

These protections reflect a "'national referendum' attesting to [the United States'] sense of the critical role that a vibrant press plays in a free society." Rodney A. Smolla, *The First Amendment, Journalists, and Sources: A Curious Study in "Reverse Federalism,"* 29 Cardozo L. Rev. 1423, 1429 (2008). Indeed, states across the country have found these laws necessary to protect the "paramount public interest" in maintaining "a vigorous, aggressive and independent press." *People v. Silverstein*, 412 N.E. 2d 692, 695 (Ill. App. Ct. 1980), *rev'd on other grounds*, 429 N.E.2d 483 (Ill. 1981) (quoting *Baker v. F&F Inv.*, 470 F.2d 778, 782 (2d Cir. 1972)) (discussing the Illinois legislature's adoption of that state's shield law). Such laws are thus "essential to [the] maintenance of our free and democratic society." *Holmes v. Winter*, 22 N.Y.3d 300, 303–09 (N.Y. 2013). At the federal level, all but two federal courts of appeals have recognized some form of a qualified privilege under the First Amendment or common law. *See Reporter's Privilege Compendium*, Part III.A, The Reporters Comm. for Freedom of the Press, https://www.rcfp.org/privilege-sections/a-generally/ (last visited Sept. 9, 2019). These laws provide a range of protections, but the broader theme is clear: forcing a journalist to disclose a confidential source is only permissible after the government has satisfied a set of stringent requirements, such as need, the centrality of the material to the matter, and the inability of investigators to get the material from a non-media source.

The government's mass surveillance at issue compromises the ability of the news media to ensure the confidentiality and anonymity of their sources. It therefore threatens the integrity of newsgathering and the ability of the press to provide unvarnished reporting on both the government and private sector. Legislatures and courts across the country have repeatedly affirmed the importance of an independent press in the promotion of an informed electorate.

B. Recent developments highlight the government's increased appetite for prosecuting the act of publishing government secrets and the chilling effect that has on reporter-source communications.

The chilling effect of mass surveillance should also be considered in light of a broader trend, which began with the Obama administration in 2009, of aggressively prosecuting government employees or contractors who have disclosed classified, or otherwise controlled, information to members of the news media. President Obama's Justice Department prosecuted at least ten cases against these "leakers," more than all previous administrations combined. *See* Gabe Rottman, *Federal Cases Involving Unauthorized Disclosures to the News Media, 1778 to the Present*, The Reporters Comm. for Freedom of the Press, https://www.rcfp.org/wp-content/uploads/2019/05/leaks-investigations-chart-gabe-rottman-may-21-2019.pdf (last visited Sept. 9, 2019); *see also* Gabe Rottman, *A Typology of Federal News Media "Leak" Cases*, 93 Tul. L. Rev. 1147, 1157–58 (2019). The current administration has already prosecuted seven leak cases, and has secured the longest

and second-longest prison sentences in these cases, with 63 months for Reality Winner, a former NSA contractor and the first person to sentenced for violating the Espionage Act under the Trump administration, and 48 months for Terry Albury, a former special agent with the FBI's Minneapolis Field Office and the second person to be sentenced for violating the Espionage Act under this administration. *See* Gabe Rottman, Federal Cases Involving Unauthorized Disclosures to the News Media, 1778 to the Present, *supra*. Most recently, the Justice Department indicted WikiLeaks founder Julian Assange on 17 counts of violating the Espionage Act for the solicitation, receipt, and publication of classified information. *See* Charlie Savage, *Assange Indicted Under Espionage Act, Raising First Amendment Issues,* N.Y. Times (May 23, 2019), https://perma.cc/T2BY-3WMC. Notably, the last three of those 17 counts describe an act of pure publication, "focusing on Assange's having posted the documents on the internet" and not "on some other action, such as encouraging the leak or receiving the information." Gabe Rottman, *The Assange Indictment Seeks to Punish Pure Publication*, Lawfare (May 24, 2019), https://perma.cc/3GQF-MHHY. This superseding indictment replaced the original indictment, which included only one count of conspiracy to violate the Computer Fraud and Abuse Act and was relatively limited in scope compared to the expansive Espionage Act charges. *See* Gabe Rottman, *Special Analysis of the May 2019 Superseding Indictment of Julian Assange,* Communications Lawyer

(2019), https://www.americanbar.org/content/dam/aba/publications/communications_lawyer/Summer2019/cl_v34_n4.pdf.

This trend has heightened anxiety among reporters and news organizations over the integrity of their communications with confidential sources, and has deterred sources and potential whistleblowers from coming forward. *See* Avi Asher-Shapiro, *Leak prosecutions under Trump chill national security beat,* Comm. to Protect Journalists (Mar. 6, 2019), https://cpj.org/blog/2019/03/leak-prosecutions-trump-national-security-beat.php (last visited Sept. 13, 2019); *see also* Editorial, *A Journalist 'Co-Conspirator,'* Wall St. J. (May 20, 2013), https://perma.cc/YS5N-S84X (discussing the Justice Department's seizure of phone records of AP reporters and editors and Fox News reporter James Rosen's emails, and observing that "[t]he suspicion has to be that maybe these 'leak' investigations are less about deterring leakers and more about intimidating the press"). With the new indictment against Assange, there are even more acute concerns that the same legal theory utilized against Assange could be used to "criminalize[] activities that are crucial to American investigative journalists who write about national security matters." Savage, *Assange Indicted Under Espionage Act, Raising First Amendment Issues*; *Reporters Committee Statement on latest Assange indictment, supra*; The Reporters Committee for Freedom of the Press statement on latest Assange indictment (May 23, 2019), https://www.rcfp.org/may-

2019-rcfp-assange-statement/ ("Any government use of the Espionage Act to criminalize the receipt and publication of classified information poses a dire threat to journalists seeking to publish such information in the public interest, irrespective of the Justice Department's assertion that Assange is not a journalist.").

While Espionage Act leak investigations are criminal, and are pursued using criminal investigative tools, information gathered in the course of the surveillance programs challenged here could still figure in criminal leak investigations.

For instance, material collected under Section 702 of the Foreign Intelligence Surveillance Act Amendments Act, Pub. L. No. 110-261, 122 Stat. 2436 (2008), codified at 50 U.S.C. § 1881a (the "FISA Amendments Act"), will be transmitted to the FBI—the agency responsible for investigating national security leaks—if it includes selectors associated with a full investigation. *See* Asha Rangappa, *Don't Fall for the Hype: How the FBI's Use of Section 702 Surveillance Data Really Works*, Just Security (Nov. 29, 2017), https://perma.cc/68B5-XBP3. That information will then be included in the FBI's Data Integration and Visualization System, or DIVS, which permits one search term to access multiple FBI databases. *Id.* A DIVS search is one of the first investigative steps the FBI will conduct at the assessment stage of a matter. *Id.* And, while 702 material is not immediately accessible to an uncleared investigator, it may be accessible at some point to cleared FBI agents. *Id.* In other words, this

system—often referred to as the FBI "backdoor"—permits U.S. person selectors to form the basis of a Section 702 search and for Section 702 material to be used in criminal investigations. *Id.*; *see also* Selina MacLaren, *How Do Leak Investigations Work?*, Lawfare (May 16, 2017), https://perma.cc/5E9L-E5H7 (explaining how a "preliminary inquiry" at an intelligence agency leads to a Justice Department leak investigation).

Additionally, several memorandums recently disclosed by the Justice Department pursuant to Freedom of Information Act litigation detail special procedures to be followed by members of the department in any investigation "targeting known media entities or known members of the media" using tools available under the original Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978), and the FISA Amendments Act. *See* Memorandum from the Att'y Gen. to the Nat'l Sec. Div. Regarding Procedures for Processing Foreign Intelligence Surveillance Act ("FISA") Applications Targeting Known Media Entities or Known Members of the Media (Mar. 19, 2015) (requiring attorney general or deputy attorney general review of FISA applications targeting members of the news media); Memorandum from the Deputy Att'y Gen. to the Nat'l Sec. Div. Regarding Guidance for Processing Foreign Intelligence Surveillance ("FISA") Applications Targeting Known Media Entities or Known Members of the Media (Jan. 8, 2015) (same). As stated in these memorandums,

the Justice Department has procedures in place for high-level review of any FISA applications targeting members of the news media. To the extent that foreign intelligence investigative tools implicate the press, such tools can chill newsgathering by dissuading sources from coming forward for fear that their identities will thus be revealed. *See* Gabe Rottman & Linda Moon, *How foreign intelligence surveillance law applies to the news media*, The Reporters Comm. for Freedom of the Press (Nov. 9, 2018), https://perma.cc/6U6A-A99N.[2]

C. The surveillance methods at issue here are especially damaging to journalism because they target content as well as metadata.

Legislatures and the courts have recognized the distinction between communication records and content by granting more protection to the content of telephone and email messages than to metadata. For instance, the section of the Electronic Communications Privacy Act ("ECPA") known as the Wiretap Act institutes enhanced requirements before law enforcement can intercept the content of telephone and electronic communications. *See* 18 U.S.C. § 2518. It requires that an application for an order authorizing the use of a wiretap demonstrate "probable cause" that one of the enumerated offenses is being committed, has been

[2] The Justice Department memorandums do not reference Section 702. Rather than tasking selectors through individual court orders, the attorney general and director of national intelligence secure annual authorization orders from the FISA court setting out the procedures by which selectors are chosen, and individual tasking is done by the collectors at the National Security Agency. 50 U.S.C. § 1881a.

committed, or is about to be committed, and provides that any evidence obtained in violation of this section can be excluded from trial. *Id.* It also requires that law enforcement show they have exhausted all other investigative tools before the use of a wiretap and use "minimization" procedures to limit interception outside the scope of the warrant. *Id.* Similarly, the Stored Communications Act distinguishes between content and metadata in terms of the applicable standards and investigative tools that can be used to compel electronic communications records. 18 U.S.C. § 2703. And, the Pen Register Act, which governs the collection of metadata concerning who communicated with whom through electronic means, provides for interception through an application containing a certification by the applicant that the information sought would be "relevant" to an ongoing criminal investigation. *See* 18 U.S.C. § 3122(b)(2).

To be clear, *amicus* believes that the indiscriminate collection of metadata harms reporter-source relationships and the newsgathering process, and it may do so to a greater degree than content collection in some cases. Content can be coded or encrypted, but metadata is harder to obscure. *See* Br. of Amici Curiae of the Reporters Comm. for Freedom of the Press and 19 Media Orgs. in Supp. of Pet'r, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402). Nonetheless, the additional protections that legislators have given to the substantive content of electronic communications only showcases the importance of protections for

reporter-source confidentiality in this case, and communications content will often include journalistic work product material, which, as discussed above, has received special protections under the laws of most states and through federal legislation such as the Privacy Protection Act. *See* 42 U.S.C. § 2000aa.

The Supreme Court has similarly recognized, as early as 1878, an elevated privacy right in the content of communications. *See Ex parte Jackson*, 96 U.S. 727 (1877) (finding searches of contents of letters unreasonable in contrast to merely looking at the writings on the outside of envelopes). Following *Ex parte Jackson*, the Court extended the Fourth Amendment protections to the content of telephone calls. *See Katz v. United States*, 389 U.S. 347, 352 (1967) (explaining that a person is "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world"). The content of communications receives this special protection because it contains an individual's "innermost thoughts." Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 Stan. L. Rev. 1005, 1018-22 (2010) (comparing email content to the inside of a person's home, which also gets heightened Fourth Amendment protection); *see also Warshak v. United States*, 631 F.3d 266, 288 (6th Cir. 2010) (finding that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails" and requiring a Fourth Amendment probable cause warrant to compel the production of the content of emails (internal citation omitted)).

It is especially important for journalists that the content of email and telephone messages remain private because that work product forms the background for and basis of investigative articles. *See, e.g.*, Norman Pearlstine, PBS Frontline Interview, PBS, https://perma.cc/A2V8-PDTD (last visited Aug. 14, 2019) (interviewing a former editor-in-chief of Time Magazine and the current executive editor of the Los Angeles Times who describes information from anonymous sources as part of the "fabric of American journalism"). The type of reporting that journalists can undertake with information from anonymous sources is "essential to a flourishing self-governing society." The President's Review Group on Intelligence and Commc'ns Technologies, *Liberty and Sec. in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Commc'ns Technologies*, 1, 127 (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (last visited Aug. 14, 2019) ("Part of the responsibility of our free press is to ferret out and expose information that government officials would prefer to keep secret when such secrecy is unwarranted."). Thus, as the Privacy and Civil Liberties Oversight Board recognized, mass surveillance programs that permit the collection of communications metadata and content present "serious repercussions today for the freedom of the press" as they sweep up

journalistic work product in addition to reporter-source communications. *Id.* at 127.

II. Mass surveillance negates the safeguards the government itself has adopted to protect reporter-source confidentiality and the independence of the press.

In direct response to the public outcry over the seizure of records from the Associated Press and another incident involving a search warrant for Fox News reporter James Rosen's personal emails, *see* Ann E. Marimow, *Justice Department's scrutiny of Fox News reporter James Rosen in leak case draws fire*, Wash. Post (May 20, 2013), https://perma.cc/U25E-9AFU, the Justice Department revised the internal guidelines that govern the collection of records or information from members of the news media in 2014 and 2015 to strengthen protections for journalists. *See* 28 C.F.R. § 50.10; *see also Strengthening and Preserving the Attorney General Guidelines for Media Subpoenas*, The Reporters Comm. for Freedom Press, https://perma.cc/T6Q4-RYEU.

The revised guidelines build upon a set of internal policies developed during the Nixon administration and promulgated by Attorney General John Mitchell, which were intended to prevent the press from becoming a "quasi-governmental investigatory agency." John N. Mitchell, *"Free Press and Fair Trial: The Subpoena Controversy" and Address* (Aug. 10, 1970), https://www.justice.gov/sites/default/files/ag/legacy/2011/08/23/08-10-1970.pdf. The guidelines reflect the

shared understanding between prosecutors and the press that newsgathering is both constitutionally protected and would be compromised without effective checks on unnecessary investigative scrutiny of the press. *See* Mitchell, *"Free Press and Fair Trial: The Subpoena Controversy" and Address*, *supra* (explaining that the "guidelines are designed to provide new and reasonable safeguards to protect the rights and privileges of a free press in a manner consistent with the 'paramount public interest in the fair administration of justice'").

The guidelines now cover most criminal investigative tools (previously they only applied to subpoenas) and deploy three key procedural safeguards to those tools to prevent the press from becoming a "government investigator." *See id*. First, most search warrants, court orders, and subpoenas to a member of the news media or for news media records from a third-party vendor require personal approval by the attorney general. 28 C.F.R. § 50.10(c)(1), (d)(1). Second, prosecutors should make "all reasonable attempts to obtain the information from alternative, non-media sources" before they can seek a search warrant, court order, or subpoena. *Id.* § (c)(4)(ii), (c)(5)(ii), (d)(3). And, third, with only limited exceptions, members of the news media must be notified before a third-party can be compelled to disclose a journalist's or news organization's records or communications to give the journalist or news organization a chance to challenge the demand in court. *Id.* § (e)(ii). As noted above, Justice Department policies

also require high-level review in foreign intelligence investigations targeting members of the news media. *See* Section I.B, *supra.*

The Justice Department's internal policies signify its commitment to handling criminal investigations affecting journalistic rights in a careful and thoughtful manner based on a particular set of circumstances, and they provide meaningful protections for newsgathering. However, the collection of journalistic work product and reporter-source communications or metadata through any of the mass surveillance programs in this case circumvents these protections and therefore contributes to the chill that undue surveillance places on sources and newsgathering.

CONCLUSION

For the foregoing reasons, *amicus* respectfully requests that the Court reverse the district court's order dated April 25, 2019, and remand the case for further proceedings.

Respectfully submitted,

/s/ Bruce D. Brown
Bruce D. Brown
Counsel of Record
Katie Townsend
Gabriel Rottman
Linda Moon
THE REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th St. NW, Suite 1020
Washington, D.C. 20005
Phone: (202) 795-9300
Fax: (202) 795-9310
bbrown@rcfp.org

Dated: September 13, 2019

CERTIFICATE OF COMPLIANCE WITH RULE 32(G)

I, Bruce D. Brown, do hereby certify that the foregoing brief of *amicus curiae*:

1) Complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because it contains 4,795 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f), as calculated by the word-processing system used to prepare the brief; and
2) 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 it has been prepared in a proportionally spaced typeface using Microsoft Office Word in 14-point, Times New Roman font.

/s/ Bruce D. Brown
Bruce D. Brown, Esq.
Counsel of Record
THE REPORTERS COMMITTEE
FOR FREEDOM OF THE PRESS

Dated: September 13, 2019
Washington, D.C.

CERTIFICATE OF SERVICE

I, Bruce D. Brown, do hereby certify that I have filed the foregoing Brief of *Amicus Curiae* electronically with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit using the appellate CM/ECF system on September 13, 2019.

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

/s/ Bruce D. Brown
Bruce D. Brown, Esq.
Counsel of Record
THE REPORTERS COMMITTEE
FOR FREEDOM OF THE PRESS

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Form 8. Certificate of Compliance for Briefs

Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf

9th Cir. Case Number(s) 19-16066

I am the attorney or self-represented party.

This brief contains 4,795 **words**, excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

- ○ complies with the word limit of Cir. R. 32-1.
- ○ is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.
- ◉ is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).
- ○ is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.
- ○ complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one):*
  - ○ it is a joint brief submitted by separately represented parties;
  - ○ a party or parties are filing a single brief in response to multiple briefs; or
  - ○ a party or parties are filing a single brief in response to a longer joint brief.
- ○ complies with the length limit designated by court order dated [ ].
- ○ is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/Bruce D. Brown **Date** September 13, 2019

*(use "*s/[typed name]*" to sign electronically-filed documents)*

Feedback or questions about this form? Email us at forms@ca9.uscourts.gov