No. 23-13649-H

IN THE UNITED STATES COURT OF APPEALS
ELEVENTH CIRCUIT

TIMOTHY BURKE v. UNITED STATES

On Appeal from the United States District Court for the Middle District of Florida, Tampa Division

No. 8:23-mc-14
Hon. Mag. J. Sean P. Flynn

BRIEF OF AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF FLORIDA, FREEDOM OF THE PRESS FOUNDATION, FLORIDA FIRST AMENDMENT FOUNDATION, FOUNDATION FOR INDIVIDUAL RIGHTS AND EXPRESSION, NATIONAL PRESS CLUB, AND NATIONAL PRESS CLUB JOURNALISM INSTITUTE AS *AMICI CURIAE* SUPPORTING APPELLANT AND REVERSAL

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
E-mail: jgranick@aclu.org
Counsel for Amici Curiae

Seth Stern*
Caitlin Vogus*
FREEDOM OF THE PRESS FOUNDATION
49 Flatbush Avenue #1017
Brooklyn, NY 11217
Tel: (510) 995-0780
E-mail: caitlin@freedom.press
seth@pressfreedomfoundation.org

*Not admitted in the Eleventh Circuit.

Esha Bhandari
Vera Eidelman
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
E-mail: ebhandari@aclu.org
vedeilman@aclu.org

Daniel Tilley
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION OF FLORIDA
4343 W. Flagler St., Suite 400
Miami, FL 33134
Tel: (786) 363-2714
E-mail: DTilley@aclufl.org

Edward L. Birk
MARKS GRAY, PA,
1200 Riverplace Blvd. Suite 800
Jacksonville, FL 32207
Tel: (904) 807-2179
E-mail: EBirk@marksgray.com
Co-Counsel for First Amendment Foundation

Ronnie London
William Creeley*
FOUNDATION FOR INDIVIDUAL RIGHTS
AND EXPRESSION
510 Walnut Street, Suite 900
Philadelphia, PA 19106
Tel: (215) 717-3473
E-mail: ronnie.london@thefire.org

Charles D. Tobin
BALLARD SPAHR LLP
1909 K Street NW, 12th Floor
Washington, DC 20006
Tel: (202) 661-2200
E-mail: tobinc@ballardspahr.com
Co-Counsel for National Press Club and National Press Club Journalism Institute

*Not admitted in the Eleventh Circuit.

CERTIFICATE OF INTERESTED PERSONS AND CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure Rule 26.1 and Eleventh Circuit Rule 26.1-1, *Amici* provide the following certificate of interested persons, in addition to those listed in the first brief filed:

Bhandari, Esha (Counsel for *Amici curiae*)

Birk, Edward (Counsel for *Amici curiae*)

Eidelman, Vera (Counsel for *Amici curiae*)

Granick, Jennifer (Counsel for *Amici curiae*)

London, Ronnie (Counsel for *Amici Curiae*)

Tilley, Daniel (Counsel for *Amici curiae*)

Tobin, Charles (Counsel for *Amici curiae)*

American Civil Liberties Union (*Amicus curiae*)

American Civil Liberties Union of Florida (*Amicus curiae*)

First Amendment Foundation (*Amicus curiae*)

Foundation for Individual Rights and Expression (*Amicus curiae*)

Freedom of the Press Foundation (*Amicus curiae*)

National Press Club (*Amicus curiae*)

National Press Club Journalism Institute (*Amicus curiae*)

Pursuant to Rule and 29(a)(4)(A) of the Federal Rules of Appellate Procedure, *amici curiae* state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

DATED this January 2, 2024

/s/ Jennifer Stisa Granick
Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
E-mail: jgranick@aclu.org

Counsel for Amici Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

REGULATIONS

STATEMENT OF INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union (ACLU) is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles of liberty and equality embodied in the United States Constitution and civil rights laws. The American Civil Liberties Union of Florida is a state affiliate of the national ACLU.

The First Amendment Foundation is a nonpartisan, nonprofit organization, based in Florida and dedicated to safeguarding and promoting the fundamental freedoms of expression recognized in the First Amendment.

The Foundation for Individual Rights and Expression (FIRE) is a nonpartisan, nonprofit organization dedicated to defending the individual rights of all Americans to free speech and free thought—the essential qualities of liberty.

Freedom of the Press Foundation (FPF) is a nonprofit organization that protects, defends, and empowers public-interest journalism.

The National Press Club is the world's leading professional organization for journalists. Founded in 1908, the Club has 3,100 members representing most major news organizations.

---

[1] Pursuant to Rule 29(a)(2), counsel for *amici curiae* state that all parties have consented to the filing of this brief. Pursuant to Rule 29(a)(4)(E), counsel for *amici curiae* certify that no person other than *amici curiae*, their members, or their counsel made a monetary contribution to the presentation or submission of this brief. No current counsel for a party authored this brief in whole or in part.

The National Press Club Journalism Institute is the non-profit affiliate of the National Press Club, founded to advance journalistic excellence for a transparent society.

INTRODUCTION AND SUMMARY OF ARGUMENT

Because of the search warrant executed in this case, journalists are rightfully concerned that the government considers routine, modern-day newsgathering techniques—including accessing unencrypted and unsecured websites—to be criminal under the Wiretap Act and the Computer Fraud and Abuse Act (CFAA). While important facts about this case are under seal, it appears that the government investigated Mr. Burke, and seized his journalist work product, after he accessed an unencrypted video stream and publicized its embarrassing and newsworthy contents. The Internet address, or URL[2], for that stream was listed on a webpage that anyone could access with a publicly available username and password. But the Department of Justice's (DOJ) legal interpretation—whether the government thinks that accessing published, unencrypted, but difficult-to-guess URLs violates the law—remains secret because the search warrant affidavit remains sealed.

If that newsgathering activity alone served as the basis for the search and seizure in this case, it would run afoul of the First Amendment. Even if there was something more, the current secrecy and resulting ambiguity will chill legitimate newsgathering. That is why over 50 organizations, including *amici*, sent a letter to

[2] The URL, or Uniform Resource Locator, is like an address for a webpage or other information transmitted over the web, and takes a form similar to www.aclu.org.

the DOJ seeking transparency about why the government believes Timothy Burke's newsgathering broke the law.[3]

This Court can address that transparency problem by ordering the probable cause affidavit unsealed, subject to necessary redactions, to reveal the government's legal theories. That way, to the extent that the investigation of Burke hinges on conduct other than routine online newsgathering, other journalists will be reassured that they can do their constitutionally protected work without fear of being raided by federal agents.

Additionally, the Court should order the government to return any seized information that is not relevant to a legitimate criminal investigation as well as the tools and instrumentalities Burke uses for his newsgathering. Burke needs his hardware to preserve his research, especially since Google recently threatened to delete his remote storage account.[4] Returning these materials is essential to preserve

[3] Press Release, Freedom of the Press Foundation, *Rights Orgs, Broadcasters Demand Info On FBI Raid Of Journalist's Home* (Oct. 4, 2023), https://freedom.press/news/rights-orgs-broadcasters-demand-info-on-fbi-raid-of-journalists-home/.

[4] Mike Masnick, *Google Promises Unlimited Cloud Storage; Then Cancels Plan; Then Tells Journalist His Life's Work Will Be Deleted Without Enough Time To Transfer The Data*, TechDirt (Dec. 12, 2023), https://www.techdirt.com/2023/12/12/google-promises-unlimited-cloud-storage-then-cancels-plan-then-tells-journalist-his-lifes-work-will-be-deleted-without-enough-time-to-transfer-the-data/.

Burke's constitutional right to engage in timely reporting. It is also required to ensure compliance with the Privacy Protection Act of 1980 (PPA) and DOJ regulations.

BACKGROUND FACTS

Timothy Burke is an investigative journalist with a history of noteworthy reporting. He broke the story that Notre Dame linebacker Manti Te'o was the victim of an elaborate online romantic hoax.[5] Burke also created an influential video essay assembling dozens of video clips of Sinclair Broadcast Group news anchors across the U.S. intoning an identical script criticizing "fake news."[6] He has served as a director of video news at The Daily Beast and Gizmodo Media Group. He has over 116,000 followers on X.com.

This case apparently arises from Burke's May 2023 reporting about an interview between Tucker Carlson, at the time an anchor with Fox News, and performer Kanye West (Ye).[7] Burke located an unedited livestream of the interview, in which Ye made unaired antisemitic and racist comments.

---

[5] Timothy Burke and Jack Dickey, *Manti Te'o's Dead Girlfriend, The Most Heartbreaking and Inspirational Story of the College Football Season, Is a Hoax*, Deadspin (Jan. 16, 2013), https://deadspin.com/manti-teos-dead-girlfriend-the-most-heartbreaking-an-5976517/.

[6]Timothy Burke, *How America's Largest Local TV Owner Turned Its News Anchors Into Soldiers In Trump's War On The Media*, Deadspin (Mar. 31, 2018), https://deadspin.com/how-americas-largest-local-tv-owner-turned-its-news-anc-1824233490/.

[7] *See* Christopher Spata, Dan Sullivan and Justin Garcia, *Tucker Carlson*, *Fox News hacks tied to FBI search of Tampa council member's home*, Tampa Bay Times (May 26, 2023),

Burke claims the livestreams were unencrypted, publicly accessible feeds. Anyone who typed the URL for these feeds into a web browser would be able to see them. Although the URLs were not published in any search engine,[8] Burke was able to see a list of them on a webpage created by a company that provides video streaming services to broadcasters. People could access this webpage with a username and password. The username and password that Burke used were posted publicly online, apparently by their owner, without any restriction on their use. The streaming service often distributed "demo" credentials for free to entities that wanted to try the service.

Fox News, according to Burke's lawyers, claimed to the Federal Bureau of Investigation (FBI) that the unedited live streams had been "hacked."[9] In May, FBI agents searched Burke's home and seized equipment and work product, as well as other documents belonging to him and his wife, Tampa Florida Councilwoman Lynn Hurtak. The government suspects Burke of violating the CFAA, 18 U.S.C. § 1030,

---

https://www.tampabay.com/news/tampa/2023/05/26/tucker-carlson-fox-news-hacks-tied-fbi-search-tampa-council-members-home/.

[8] A software program is capable of guessing many URLs in rapid succession, which can reveal Internet-published information without the user relying on a search engine to have indexed the URL or having prior knowledge of that website address.

[9] Bobby Block, *First Amendment Foundation: Raids On Journalists Put Free Expression Under Siege*, Palm Beach Post (Aug. 19, 2023), https://www.palmbeachpost.com/story/opinion/columns/2023/08/19/police-fbi-law-enforcement-raids-journalists-florida-kansas-illegal-first-amendment-privacy-act/70619490007/.

and of unlawfully intercepting electronic communications in violation of the Wiretap Act, 18 U.S.C. § 2511. Search Warrant Record #1 Ex. 1, ECF No. 18-1.

Burke moved to unseal the warrant and related materials. The Tampa Bay Times intervened to urge the same. Mot. to Intervene 1-2, ECF No. 1. The district court unsealed redacted versions of the search warrant records but denied the motion to unseal the affidavit supporting the search warrant, a document which would reveal *why* Burke was investigated. Search Warrant Record #1 Ex. 1, ECF No. 18-1. It cited concern over revealing details of the government's investigation.

Burke also asked under Federal Rule of Criminal Procedure 41 for the government to return his property. The district court treated that motion as a request to exercise equitable jurisdiction and applied the test from *Richey v. Smith*, 515 F.2d 1239 (5th Cir. 1975). The court found that Burke did not meet the relevant *Richey* factors, in particular because the government did not show "callous disregard" for Burke's First Amendment rights. It noted that, to obtain the warrant, the government would have had to establish probable cause to believe that Burke's home contained the fruits, instrumentalities, and/or evidence of violations of 18 U.S.C. § 1030 and 18 U.S.C. § 2511.

ARGUMENT

I. The First Amendment protects modern journalism involving the collection of information from publicly available sources online, including by accessing obscure URLs.

The First Amendment protects the vital role journalism plays in keeping powerful institutions accountable to the public. *New York Times Co. v. United States* (Pentagon Papers), 403 U.S. 713, 714 (1971) (per curiam); *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964). "[S]tate action to punish the publication of truthful information seldom can satisfy constitutional standards." *Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 102 (1979). And "if a newspaper lawfully obtains truthful information about a matter of public significance, then state officials may not constitutionally punish publication of the information, absent a need . . . of the highest order." *Id.* at 103; *see also Florida Star v. B.J.F.*, 491 U.S. 524 (1989); *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829 (1978).

The same is true for gathering news. "[E]ntrenched in Supreme Court case law is the principle that the First Amendment's protections for free speech include a constitutionally protected right to gather news." *Nicholas v. Bratton*, 376 F. Supp. 3d 232, 279 (S.D.N.Y. 2019). "Without some protection for seeking out the news, freedom of the press could be eviscerated." *Branzburg v. Hayes*, 408 U.S. 665, 681 (1972). Indeed, "[t]he protected right to publish the news would be of little value in

the absence of sources from which to obtain it." *CBS, Inc. v. Young,* 522 F.2d 234, 238 (6th Cir. 1975).

"The right to gather information plays a distinctly acute role in journalism," *People for the Ethical Treatment of Animals, Inc. v. N.C. Farm Bureau Fed'n, Inc*., 60 F.4th 815, 829 (4th Cir. 2023) (Petition for Cert. Filed, Nos. 22-1148 & 22-1150, (May 26, 2023), and the First Amendment "undoubted[ly]" protects the "right to gather news from any source by means within the law." *Glik v. Cunniffe*, 655 F.3d 78, 82 (1st Cir. 2011) (internal quotation marks and citation omitted). This extends to any information that is made public, whether intentionally or inadvertently, and it reaches even "surreptitious, confrontational, unscrupulous, and ungentlemanly" newsgathering methods. *J.H. Desnick v. Am. Broad. Cos., Inc*., 44 F.3d 1345, 1355 (7th Cir. 1995).

Those seeking to inform the public have a right to engage in "routine newspaper reporting techniques," *Smith*, 443 U.S. at 103, and they are even entitled to procure and publish materials from sources who obtained them illegally, *Bartnicki v. Vopper*, 532 U.S. 514 (2001). This holds with equal force for independent and freelance journalists. Courts have rightly warned against limiting First Amendment protections to established media outlets, *see, e.g., Pulliam v. County of Fort Bend*, No. H-22-4210, 2022 WL 19929594 (S.D. Tex. June 30, 2023); *Von Bulow by*

Auersperg v. Von Bulow, 811 F.2d 136 (2d Cir. 1987)—a warning that is especially important as technological advances give rise to new forms of journalism.[10]

Because so much communication now takes place on the Internet, many news sources are found online. Website operators and users routinely expose newsworthy information to the public, either without intending to or with the expectation that no one will notice. Just as routinely, journalists, academics, and other researchers use a range of techniques to uncover and report that information.

For example, in 2021, The Intercept's Mara Hvistendahl obtained a series of slide decks describing how Oracle markets its products for use in Chinese surveillance.[11] She found them by running a Google search for relevant Chinese characters, which returned links to the slide decks on Oracle's website, even though Oracle seemed to be unaware that the documents were accessible.[12]

In another example, an independent researcher obtained information regarding the January 6th attack on the Capitol Building by accessing supposedly "hidden" but publicly accessible URLs on the social media site Parler. Though users

---

[10] Margaret Sullivan, *Every week, two more newspapers close — and 'news deserts' grow larger*, Wash. Post (June 29, 2022), https://www.washingtonpost.com/media/2022/06/29/news-deserts-newspapers-democracy/.

[11] Mara Hvistendahl, *How Oracle Sells Repression in China*, The Intercept (Feb. 18, 2021), https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.

[12] Grayson Clary, *California city backs down from misguided 'hacking' lawsuit against bloggers,* Reporters Committee for Freedom of Press (May 26, 2021), https://www.rcfp.org/fullerton-ca-drops-hacking-lawsuit/.

thought they had deleted the content, Parler continued to host it at addresses that anyone could visit, on a series of sequential URLs, in the order that each piece had been posted. Once obtained by the researcher, this data formed the basis for a ProPublica analysis of live video from January 6[13] and a detailed Gizmodo map of the location metadata tied to those posts.[14]

In the physical world, it is unremarkable that journalists might gain access to information in ways that offend the subjects of their reporting—seeing a document unintentionally left out in public, for example, or overhearing a conversation at a crowded restaurant. In rare cases, this access might be legally problematic—if a reporter participated in theft of the materials, for example. But for the most part, these activities are familiar and accepted. This should also be true online, at least with respect to information that is publicly available, and which the newsgatherer himself could not reasonably be deemed to have unlawfully obtained. *See Bartnicki*, 532 U.S. at 535.

---

[13] Alec MacGilis, *Inside the Capitol Riot: What the Parler Videos Reveal*, ProPublica (Jan 17, 2021), https://www.propublica.org/article/inside-the-capitol-riot-what-the-parler-videos-reveal/.

[14] Dell Cameron and Dhruv Mehrotra, *Parler Users Breached Deep Inside U.S. Capitol Building, GPS Data Shows,* Gizmodo (Jan. 12, 2021), https://gizmodo.com/parler-users-breached-deep-inside-u-s-capitol-building-1846042905/.

II. The breadth and vagueness of the CFAA and the Wiretap Act can chill First Amendment protected newsgathering activities, particularly where (as here) the government keeps its rationale for potential charges secret.

A. The government appears to be interpreting the CFAA in a dangerously overbroad manner despite Supreme Court case law warning against overreach.

The CFAA criminalizes accessing (1) a computer (2) "without authorization" or by "exceed[ing] authorized access" and (3) thereby obtaining information or causing damage or loss. *See* 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(5)(C). The CFAA definition of "computer" encompasses "effectively all computers with Internet access." *United States v. Nosal*, 676 F.3d 854, 859 (9th Cir. 2012). And the requirement of damage or loss is not necessarily a meaningful discriminator between what most people would consider permissible and illegal conduct.[15] Therefore, how the government defines "authorization" determines the difference between lawful behavior and potential crimes.[16]

For many years, the DOJ pushed the view that the CFAA could cover accessing electronically-stored information for a purpose adverse to the computer owner's interests, even if the access did not bypass technological barriers or

---

[15] *See* Jennifer S. Granick, *Faking it: Calculating Loss in Computer Crime Sentencing*, 2 I/S - A Journal of Law and Policy for the Information Society 2 (Spring/Summer 2006) (arguing that loose definitions of "damage" and "loss" fail to discriminate between harmful and trivial access to computer systems).

[16] Similar to the CFAA, liability for access to electronic communications under the Stored Communications Act, 18 U.S.C. § 2701, also hinges on the definition of "access[ing] without authorization" or "exceed[ing] authorization".

otherwise "break and enter." *See, e.g., Van Buren v. United States,* 141 S.Ct. 1648, 1660 (2021) (government asserting that the CFAA is violated when someone accesses a computer with authorization but for purposes to which such authorization does not extend). Under this reading, employees who download work-related files before quitting their jobs could be accused of illegally exceeding authorization, even if the information were non-confidential. *Van Buren,* 141 S.Ct. at 1655. So, too could employees who read the news using their work computers in violation of policies prohibiting personal use of such resources. *Id.* at 1661.

The Supreme Court rejected this interpretation in *Van Buren.* Holding that the defendant police officer did not "exceed authorized access" by accessing license plate information for an improper purpose, the Court rejected the government's argument that disloyal computer uses or violations of policies constitute "unauthorized access" under the CFAA. *Id.* at 1662. The Court explained that such a theory would attach "criminal penalties to a breathtaking amount of commonplace computer activity." *Id.* Because most websites and other services authorize access only upon an agreement to follow specified terms of service, "millions of otherwise law-abiding citizens [would become] criminals…if the 'exceeds authorized access' clause encompasses violations of circumstance-based access restrictions …" *Id*. at 1661. That, the Supreme Court held, the CFAA could not be interpreted to do.

And yet, if the government's investigation in this case is premised on Burke's access to the Fox News livestreams, it appears to continue to apply the CFAA in an overly broad manner. What the public knows about this investigation raises reasonable—and, for those engaged in newsgathering, critical—questions about whether the government deems use of a computer to collect publicly available information to be a CFAA violation if the person who posted the information does not want it to be accessed.

B. The government appears to be reading the Wiretap Act in a way that would make access to and distribution of publicly available information a crime, thereby chilling First Amendment-protected online newsgathering.

The Wiretap Act prohibits intentionally intercepting or disclosing wire, oral, or electronic communications. The statute defines "electronic communications" very broadly, including "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . " 18 U.S.C. § 2510(12). But it does not apply to systems that are configured so that their communications are "readily accessible to the general public." 18 U.S.C. § 2511(2)(g).

The statute defines "readily accessible to the general public" only as to radio communications. It is not clear how that definition applies to electronic communications, which presumably would include the video streams at issue here.

Compare In re Innovatio IP Ventures, LLC Patent Litigation, No. 11-9308, 2013 WL 5593609 (N.D. Ill. Aug. 22, 2012) (holding that unencrypted Wi-Fi is accessible to the general public) *with Joffe v. Google, Inc.*, 746 F.3d 920 (9th Cir. 2013) (holding that the Wiretap Act applies to unencrypted Wi-Fi-transmitted communications). This ambiguity leaves the public guessing whether the federal government deems accessing information from URLs that are publicly available, even if unintentionally so, a violation of the Wiretap Act.

In civil cases, some litigants have claimed that a URL is "non-public" when it has not been indexed by a search engine or otherwise published or shared. Scholars disagree, arguing that "[a] hard-to-guess URL is still a URL, and the information posted at that address is still posted and accessible to the world." Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1164–65 (2016). Courts have taken different sides in this debate. In a recent civil case brought under the CFAA, for example, the district court held that—although it was a "close call"—a URL that was inadvertently disclosed but could not have been guessed was not "readily accessible" to the general public. *Greenburg v. Wray*, No. 22-00122, 2022 WL 2176499 at *2 (D. Ariz. June 16, 2022). In contrast, in another civil case brought under the Wiretap Act and the Stored Communications Act, the court distinguished *Greenburg* and held that communications in a private Facebook group were "readily accessible to the general public" because others could apply to and be accepted into

the group. *Davis v. HDR Incorporated,* 652 F. Supp. 3d 1087, 1096 (D. Ariz. 2023). Criminal cases brought by the government do not clarify. In *United States v. Auernheimer*, the government filed criminal charges regarding access to "hard to guess" URLs. 748 F.3d 525 (3d Cir. 2014). There, the defendant had used web scraper software to identify URLs that the computer owner, AT&T, had not expected people to find. *Id.* at 530–31. The Third Circuit decided the case on venue grounds, leaving open the question of whether the information available at these URLs was "public" or not. *Id.* at 541.

What is currently publicly known about this case only adds to the confusion. In this case, anyone with the URL could have viewed the videos—the content was not encrypted or otherwise secured, and the username and password that allowed access were not only published online, but also handed out more generally in the form of demo accounts.

C. Journalists have good reason to fear the DOJ's interpretations of the CFAA and the Wiretap Act because these laws have been used in the past to silence journalists for their critical coverage of important issues of the day.

The public needs to know whether the DOJ decided to search Burke's home and newsroom, and to threaten him with criminal prosecution over a contested and unsettled interpretation of federal statutes. It would be alarming if the government were using a case involving constitutionally protected journalism that ultimately

revealed highly newsworthy information as a test case for novel and controversial legal theories. If there is more to the story that explains the government's decision to investigate Burke, the public needs to know, so journalists can continue reporting without fear of investigation or prosecution.

The fear that the government may be misusing the CFAA and Wiretap Act is unfortunately a reasonable one. Entities that want to keep secrets, including improperly, have used the vague language of hacking and wiretap statutes to threaten reporters who find newsworthy information online.

For example, in 2020, the city of Fullerton, California was using a Dropbox account to field public records requests. Though the relevant folder was accessible without a password to anyone who visited the URL, it contained documents that the city intended to keep secret.[17] Friends for Fullerton's Future, a local news blog, downloaded newsworthy documents from the folder and published them. In response, the city sued the reporters, arguing that accessing the Dropbox violated state and federal anti-hacking laws. The city claimed the reporters had not been given permission to access the documents because the URL for the Dropbox was not published on the city website.[18] Initially a judge issued a restraining order preventing

[17] *City of Fullerton v. Friends for Fullerton's Future*, No. G044597, 2012 WL 2395554 at *8 (Cal. Dist. Ct. App. June 26, 2012).
[18] Grayson Clary, *California city backs down from misguided 'hacking' lawsuit against bloggers,* Reporters Committee for Freedom of Press (May 26, 2021), https://www.rcfp.org/fullerton-ca-drops-hacking-lawsuit/.

the blog from publishing the documents. For months, this prior restraint was in effect while the reporters' legal bills mounted. Eventually, in January of 2021, the city dropped the suit and retracted "any and all assertions" that the defendants had "acted illegally in accessing the documents."[19]

In Missouri, a reporter for the St. Louis Post-Dispatch discovered a serious flaw in a state website that put thousands of Social Security numbers at risk. He alerted the state agency so it could fix the issue before he published the story. Instead of thanking him, the Missouri governor called for a criminal investigation under state computer crime laws. That case ended with a thorough rebuke of the governor by the local prosecutor, who declined to press charges, but not before the reporter spent four months with criminal charges hanging over his head. An exhaustive state report found no evidence of criminality. The prosecutor said the law was so vague that it could be abused to criminalize using "a computer to look up someone's information."[20]

---

[19] Aaron Mackey, *Victory! California City Drops Lawsuit Accusing Journalists of Violating Computer Crime Law,* Elec. Frontier Found. (May 14, 2021), https://www.eff.org/deeplinks/2021/05/victory-california-city-drops-lawsuit-accusing-journalists-violating-computer/.

[20] Jason Hancock, *Claim That Reporter Hacked State Website Was Debunked. Parson Still Says He's A Criminal*, Missouri Independent (Feb. 23, 2022), https://missouriindependent.com/2022/02/23/claim-that-reporter-hacked-state-website-was-debunked-parson-still-says-hes-a-criminal/.

And earlier this year, scandal erupted when police officers in Marion, Kansas raided the newsroom of the Marion County Record and the home of its publisher to seize computers, cellphones and documents. Records show police believed the paper broke state law in using the Internet to confirm a tip from a source about a local restauranter's DUI history.[21] Investigators apparently believed the paper's reporter violated Kansas computer crime laws by checking a box to represent that she was authorized under the Driver Privacy Protection Act (DPPA) to access driving records, even though the DPPA authorizes research. 18 U.S.C. § 2721(b)(5).[22]

Following a huge public outcry, the prosecutor withdrew the search warrant, citing insufficient evidence. Nevertheless, the raid severely hampered publication of the Record and understandably scared reporters around the country.[23] It later emerged that the paper had been investigating the police chief who spearheaded the raid, and who later resigned due to the scandal.[24]

---

[21] Jeanna Kuang, *Missouri Prosecutor Declines To Charge St. Louis Post-Dispatch Reporter Parson Targeted,* The Kansas City Star (Jul. 18, 2022), https://www.kansascity.com/news/politics-government/article258315738.html.
[22]Cyndi Fahrlander and Angie Ricono, *Affidavits Filed For Police Raid Of Marion County Record Released*, KCTV5 (Aug. 20, 2023), https://www.kctv5.com/2023/08/20/affidavits-filed-police-raid-marion-county-record-released/.
[23]Farhlander and Ricono, *supra* note 22.
[24] Tim Cushing, *Police Chief Who Headed Raid Of Kansas Newspaper Resigns Rather Than 'Defend His Actions'*, TechDirt (Nov. 7 2023), https://www.techdirt.com/2023/11/07/police-chief-who-headed-raid-of-kansas-newspaper-resigns-rather-than-defend-his-actions/.

These cases highlight a history of powerful people, motivated by embarrassment, using vague and sweeping computer crime laws to threaten press freedoms. Broad interpretations of these laws—whether by investigators, appellate courts or magistrate judges issuing search warrants—invite abuses of power and intimidate reporters and suppress reporting. Such investigations have left journalists uncertain about whether they can be prosecuted for routine newsgathering on the mistaken grounds that they violated hacking or wiretap laws.[25]

There is significant public interest in Burke's case, which has only been magnified following the national outrage over the Marion raid.[26] Without public access to the warrant affidavit, journalists are left to assume that finding information powerful people do not want found might lead to a federal investigation. To avoid chilling important and lawful investigative reporting, the affidavit must be unsealed, so that the public can understand when the DOJ considers online newsgathering violative of the CFAA or other federal laws.

Even if the government is prosecuting Burke for something other than obtaining publicly available information, the uncertainty around this investigation is

---

[25] Bruce D. Brown & Gabe Rottman, *Claiming a 'computer crime' shouldn't give police a free pass to raid newspapers*, L.A. Times (Aug. 31, 2023), https://www.latimes.com/opinion/story/2023-08-31/kansas-newspaper-raid-marion-county-record-computer-crime/; *see also* Jon Brodkin, *Missouri governor rebuffed: Journalist won't be prosecuted for viewing HTML*, Ars Technica (Feb. 14, 2022), https://arstechnica.com/tech-policy/2022/02/missouri-governor-rebuffed-journalist-wont-be-prosecuted-for-viewing-html/; Mackey, *supra* note 29.

chilling newsgathering, for "the threat of sanctions may deter . . . almost as potently as the actual application of sanctions." *National Ass'n for Advancement of Colored People v. Button,* 371 U.S. 415, 433 (1963). For that reason alone, the affidavit should be unsealed, with any redactions necessary to protect individual privacy, sources, or other sensitive information.

In addition, the affidavit will, presumably, shed light on whether the court was informed that Burke was a journalist—and whether the government considered him to be one. As discussed in further detail below, federal policy requires that the government provide journalists notice before any search of their newsgathering materials or work product occurs, and no such notice was given here.

---

[26] *See, e.g.,* Rachel Olding & Lachlan Cartwright, *FBI Raid on Journo's Home Reportedly Related to Embarrassing Tucker Carlson Vids*, Daily Beast (May 26, 2023), https://www.thedailybeast.com/raid-on-journalist-tim-burkes-home-related-to-tucker-carlson-videos-report/; Jack McCordick, *FBI Raid of Tampa Journalist Connected to Tucker Carlson Leaked Clips*, Vanity Fair (May 27, 2023), https://www.vanityfair.com/news/2023/05/tucker-carlson-leaks-fbi-investigation-tampa-journalist/; Justin Garcia, *Tim Burke and lawyers deny hacking Fox News, demand return of devices*, Tampa Bay Times (July 21, 2023), https://www.tampabay.com/news/tampa/2023/07/21/tim-burke-tucker-carlson-fox-news-hack-fbi-search/; Steven Lee Myers & Benjamin Mullin, *Raid of Small Kansas Newspaper Raises Free Press Concerns*, N.Y. Times (Aug. 13, 2023), https://www.nytimes.com/2023/08/13/business/media/kansas-marion-newspaper-police-raid.html/; Kim Zetter, *Did a Journalist Violate Hacking Law to Leak Fox News Clips? The Government Thinks He Did*, Zero Day (Aug. 17, 2023), https://www.zetter-zeroday.com/p/did-a-journalist-violate-hacking/.

D. The public is entitled under the common law to see the warrant affidavit, with any redactions necessary to protect individual privacy, sources, or other sensitive information.

The public's common-law right of access requires the same result. The general presumption under the common law is that "the public has a right of access to judicial materials." *In re Avandia Mktg., Sales Pracs. & Prods. Liab. Litig.*, 924 F.3d 662, 672 (3d Cir. 2019). This right "promotes public confidence in the judicial system by enhancing testimonial trustworthiness and the quality of justice dispensed by the court." *Id.* (quoting *Littlejohn v. BIC Corp.*, 851 F.2d 673, 678 (3d Cir. 1988)).

"Courts have uniformly held that the party seeking to have court documents restricted from public access has the burden of establishing that the presumption of public records should be overcome, and that the burden is a heavy one." *Lipocine Inc. v. Clarus Therapeutics, Inc.*, No. 19-622, 2020 WL 4569473, at *3 (D. Del. Aug. 7, 2020) (collecting cases). The opponent of access must show that the "material is the kind of information that courts protect and that disclosure will work a clearly defined and serious injury to the party seeking disclosure." *Avandia*, 924 F.3d at 672 (quoting *Miller v. Ind. Hosp.*, 16 F.3d 549, 551 (3d Cir. 1994)).

This Court can accommodate the government's concerns about revealing investigative details through redactions. Disclosing the basis for an investigation does not automatically harm government interests. To the contrary, it would serve the government's interest in enhancing public trust in the criminal process, and in

ensuring that reporting in the public interest can continue uninhibited. The public needs to know whether the government views the kind of online newsgathering at issue here as legitimate. It is hard to say that the risk of public accountability is a harm justifying judicial secrecy.

Moreover, any harm to the government's investigation is waning every day. Prosecutors have had ample time since May 2023, when they executed the search warrant, to pursue whatever avenues they believe necessitated sealing. To the extent that the affidavit includes information that, if revealed, would compromise ongoing police work regarding other suspects, that information can be redacted while ensuring that journalists and the public learn whether officials view gathering publicly-available information using electronic means as unlawful.

III. The government should return seized materials that are not related to the case and should copy or otherwise allow access to materials that enable Burke to fulfill his newsgathering function.

Amici do not have access to information regarding the specific materials seized from Burke that have yet to be returned or why specific items were seized, but Burke has contended that the seizure far exceeded what was permitted by the warrant. Even assuming the government is investigating a crime unrelated to newsgathering, and that some limited seizure is permissible, exacting care must be taken to ensure that no more newsgathering material is withheld from Burke than is absolutely necessary, and that it is withheld for no longer than necessary. It does not

appear that the government has taken Burke's newsgathering activities into account in conducting this investigation. That failure demonstrates "callous disregard" for Burke's First Amendment rights, and Burke has met the standard for return of his property under the *Richey* test.

A. Constitutional law and federal policy require that seizures of materials related to newsgathering be limited.

The First Amendment's "chief purpose" is to prevent "previous restraints upon publication." *Near v. Minnesota ex rel. Olson, Co. Atty*, 283 U.S. 697, 713 (1931). Delays in publication, like "[t]he loss of [any] First Amendment freedoms," even if they last "for . . . minimal periods of time, unquestionably constitute[] irreparable injury." *Elrod v. Burns*, 427 U.S. 347, 373-74 (1976).

Because seizures of materials related to newsgathering run "[t]he risk of prior restraint," they cannot be justified by probable cause alone. *Fort Wayne Books Inc., v. Indiana*, 489 U.S. 46, 63 (1989) (citing authorities). Instead, the Fourth Amendment's warrant requirement must be applied with "scrupulous exactitude" when the government seeks journalists' constitutionally protected newsgathering materials. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978). And the government must not interfere with timely publication of news or rummage through reporters' files. *Id.* at 566.[27]

[27] The government claims that a team was assigned to filter privileged materials seized from Burke's home. Rep. to Mot. for Req. for Oral Arg. 3, ECF No. 33. The

The First Amendment additionally requires that, in the rare event that they're permissible at all, infringements on journalists' ability to report news be narrowly tailored, in terms of both scope and duration. *See Buckley v. Valeo*, 424 U.S. 1 (1976) (requiring "exacting" scrutiny, even for "indirect[]" infringements). For example, the D.C. Circuit has held that a "full field investigation" carried out against a library employee violated the First Amendment because the expansive inquiry was not the least restrictive means available to investigate the alleged wrongdoing. *Clark v. Library of Congress*, 750 F.2d 89, 92-95 (D.C. Cir. 1984). And the Second Circuit dramatically scaled back a government agency subpoena because its scope would have impaired the First Amendment right of members of the targeted union. *Local 1814 v. Waterfront Commission of N.Y. Harbor*, 667 F.2d 267, 270 (2d Cir. 1981).

Federal law further bolsters this protection. Despite *Zurcher*'s limitations on newsroom searches and seizures, Congress was so disturbed that the Supreme Court allowed a search at all that it passed the Privacy Protection Act (PPA) in response. S. Comm. on the Judiciary, 96th Cong., S. Rep. No. 96-874 (July 28, 1989). In recognition of the constitutionally-protected role of newsgathering, the PPA makes it unlawful to "search for or seize any work product materials possessed by a person

---

government has not publicly explained how this process worked. Particularly given the government's baseless denials that Burke is a journalist (Rep. to Mot. for Req. for Oral Arg. 12, ECF No. 33), it is unclear whether it even included filtering of journalist-source communications as opposed to other potentially privileged materials, such as communications relating to Burke's wife's political office.

reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication, in or affecting interstate or foreign commerce," except when investigating crimes *unrelated* to the "receipt, possession, communication, or withholding of such materials or the information contained therein." 42 U.S.C. § 2000aa(a)-(b).

Additionally, the DOJ's "Policy Regarding Obtaining Information from or Records of Members of the News Media; and Regarding Questioning, Arresting, or Charging Members of the News Media" (the News Media Policy) states that, subject to limited exceptions, the DOJ will not "use compulsory legal process [including search warrants] for the purpose of obtaining information from or records of members of the news media acting within the scope of newsgathering." 28 C.F.R. § 50.10(a)(2). The News Media Policy states that "[a]ll authorizations pursuant to this section must comply" with the PPA. 28 C.F.R. § 50.10(q). It includes a presumption that affected journalists will be notified before the department attempts to seize their records, with very limited exceptions. 28 C.F.R. § 50.10(j). This presumption can be overcome only when "the Attorney General determines that, for compelling reasons, such notice would pose a clear and substantial threat to the integrity of the investigation, risk grave harm to national security, or present an imminent risk of death or serious bodily harm." 28 C.F.R. § 50.10(g)(ii). Notice provides journalists

the opportunity to assert their rights before the government seizes any data or documents. Burke did not receive notice.

B. The government has minimized the importance of safeguards it originally touted as meaningful protections for reporters, raising important questions about whether it is following rules journalists rely on.

The PPA, News Media Policy, and the First Amendment should all inform the Court's analysis of whether the government was permitted to search and seize Burke's newsgathering materials, as well as the permissible scope and duration of any interference with Burke's newsgathering. Instead, the government attempts to reduce the PPA and News Media Policy to procedural technicalities, arguing about whether they create standalone defenses. Rep. to Mot. for Req. for Oral Arg. 15, ECF No. 33. The government's myopic focus ignores the constitutional impetus for both the PPA and News Media Policy, which recognize that newsgathering records are protected from seizure by the First Amendment in addition to the Fourth. *See* 28 C.F.R. § 50.10(a)(1) ("Because freedom of the press can be no broader than the freedom of members of the news media to investigate and report the news, the Department's policy is intended to provide protection to members of the news media.").

Further, while the government has vaguely claimed that it fully complied with the News Media Policy, it is unclear whether that is because the government concluded that the Policy does not apply to Burke at all, or because it believes an

exception in the policies permitted the search and seizure of Burke's work product and documentary materials.[28]

The possibility that the government might not have considered Burke to be protected by the News Media Policy is especially worrisome. In the court below, the government took the position that Burke should not be considered a "member of the news media" who is "acting within the scope of newsgathering," despite the fact that the court had twice rightly acknowledged Burke's status as a member of the media.[29] In support of its position, the government claimed that Burke had not recently published under his own byline, does not work for an established media outlet, and sometimes used job titles other than "journalist."

Of course, one does not need to work full-time as a journalist to engage in protected journalism. The PPA protects anyone "with a purpose to disseminate" information to the public, regardless of whether their own byline is attached. It is quite common for journalists—including freelancers, producers, researchers, editors, news services, and consultants—to provide research and documents for stories they do not themselves write. That does not deprive them of constitutional protection. Nor would the fact that they primarily gather information from online

[28] The district court, in its order denying Burke's motion to unseal, appears to take the government at its word that it complied with the policy without questioning the basis for its representation. Order Den. Mot. to Unseal 12 n.6, ECF No. 35

[29] Order Den. Mot. to Unseal 3, ECF No. 23; Order Den. Mot. to Unseal 1, ECF No. 35.

sources. There is substantial public interest in disclosing how the government determines who is and is not a journalist, particularly given the troublingly irrelevant factors it cited to the court below.

CONCLUSION

For the foregoing reasons, this Court should unseal the search warrant materials in this case, with any necessary redactions, and order the government to return seized materials unrelated to any legitimate investigation, while also providing Burke access to seized items that enable his ongoing newsgathering.

DATED this January 2, 2024

Respectfully Submitted,

/s/Jennifer Stisa Granick

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
E-mail: jgranick@aclu.org
Counsel for Amici Curiae

Esha Bhandari
Vera Eidelman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2500
E-mail: ebhandari@aclu.org
vedeilman@aclu.org

Daniel Tilley
AMERICAN CIVIL LIBERTIES
UNION OF FLORIDA
4343 West Flagler St., Suite 400
Miami, FL 33134
Tel: (786) 363-2714
E-mail: DTilley@aclufl.org

Edward L Birk
MARKS GRAY, PA
1200 Riverplace Blvd. Suite 800
Jacksonville, FL 32207
Tel: (904) 807-2179
E-mail: EBirk@marksgray.com
Counsel for First Amendment Foundation

Ronnie London
FOUNDATION FOR INDIVIDUAL RIGHTS AND EXPRESSION
510 Walnut Street, Suite 900
Philadelphia, PA 19106
Tel: (215) 717-3473
E-mail: ronnie.london@thefire.org

Charles D. Tobin
BALLARD SPAHR LLP.
1909 K Street NW, 12th Floor
Washington, DC 20006
Tel: (202) 661-2200
E-mail: tobinc@ballardspahr.com
Counsel for National Press Club and National Press Club Journalism Institute

CERTIFICATE OF COMPLIANCE

1. This document complies with the word limit of Fed. R. App. P. 29(a)(5) and 32(a)(7) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f) this document contains 6397 words.

2. This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this document has been prepared in a proportionally spaced typeface, 14-point Times New Roman, using word processing system Microsoft Word 2019.

DATED this January 2, 2024 /s/Jennifer Stisa Granick

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
Tel: (415) 343-0758
E-mail: jgranick@aclu.org
Counsel of Record for Amici Curiae