

**UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION**

IN RE: CONTENTS OF TIMOTHY BURKE’S NEWSROOM UNLAWFULLY SEIZED BY FBI AGENTS ON MAY 9, 2023	Case No.
---	-----------------

**MOTION TO UNSEAL SWORN AFFIDAVIT AND FOR RETURN OF
THE CONTENTS OF TIMOTHY BURKE’S NEWSROOM
UNLAWFULLY SEIZED BY THE FBI
RULE 41(g) F.R.CRIM. P.**

Investigative journalist TIMOTHY BURKE files this Motion to Unseal the Sworn Affidavit and pursuant to Rule 41(g)¹ of the Federal Rules of Criminal Procedure, for the immediate return of the contents of his newsroom, including computers, mobile telephones, servers, hard drives, any other electronic devices, and any and all information and data copied, reproduced or retained therefrom that was seized from him on May 9, 2023, because the items were seized and are retained in violation of law.

The government’s warrant indicates they were investigating violations of 18 USC 1030, the Computer Fraud and Abuse Act, the criminal “hacking” statute, (hereinafter “CFAA,”) and unlawful interceptions of electronic communications in violation of 18 USC 2511, the “wiretap” statute. However, in this case, there was no

¹ Rule 41(g) provides, “A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property’s return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.”

“hacking” and there was no unlawful “interception.” Mr. Burke simply obtained public information, and reported on a matter of public concern. The government has nevertheless shut him down, seized his materials, and still retains his privileged information for examination in a manner that can only be described as a “callous disregard” for his Constitutional rights. Immediate return of all the seized items and all copies thereof is necessary.

I. Introduction

This case arose from Mr. Burke’s reporting about an edited interview between Fox News’ Tucker Carlson and Kanye West (“Ye”).² Mr. Burke obtained a copy of the full live stream of the interview (unedited), in which Ye made anti-semitic and racist comments -- comments which were edited out of the Fox broadcast. Other media outlets broadcast these live stream videos, and other videos of similarly edited sexist and disturbing comments by Carlson found by Mr. Burke.³ Carlson was subsequently fired by Fox News. For its part, Fox News falsely claimed that the unedited live streams had been “hacked,” and that they had been unlawfully “intercepted” in violation of law. When Fox News was apparently unable to uncover the source of their claimed “leaks” or “hacks” they apparently

² Without access to the affidavit in support of the warrant, the representations about why the government seized his computers are based on both news reports and conversations with the government. See, e.g., Jack McCordick, FBI Raid of Tampa Journalist Connected to Tucker Carlson Leaked Clips, Vanity Fair, May 27, 2023, available at <https://www.vanityfair.com/news/2023/05/tucker-carlson-leaks-fbi-investigation-tampa-journalist> noting that Burke “was known for having “a reputation as somebody who finds things.”

³<https://newrepublic.com/post/172487/fox-begs-media-matters-stop-publishing-tucker-carlson-videos>

outsourced their investigation to the FBI.

No leaks or hacking occurred. With respect to the Fox News live streams, the streams themselves were unencrypted, Internet addressable, publicly accessible feeds open to anyone who put a URL into a browser. No userid or password were required, and no Terms of Service breached. Mr. Burke learned of the Internet location (the URL) of the feed by using a “demo” credential *posted publicly online by the owner of the credential* and not by any unauthorized person. This provided authorized access to a website used by streaming content providers to host their content. The hosting website (“Website 1”) automatically delivered to any user -- including users of their free demo service⁴ -- lists of the URL’s of all live streams hosted on the service, including the URL for the Fox News live stream. However, access to these live streams was not restricted to users of the site, and the streams themselves were public. As noted *infra*, Mr. Burke found other live stream videos through simple searches online for URLs containing notations that they are live feeds. The Fox News live feeds - like all live feeds collected and stored by Burke -- are publicly addressable, Internet accessible, unencrypted broadcasts

⁴ In an effort to promote a SaaS product or service, companies often provide “demonstration” accounts to clients or prospective clients as a way for these customers to “try before they buy” the product or online service. <https://www.getbeamer.com/blog/free-trial-vs-demo-for-saas> (“Most SaaS companies use some variation of a free trial or a demo to help sell the product and onboard customers”). These demo accounts permit lawful access to the product or service, and are frequently shared among those who wish to try a service. The account credentials (userid and password) for demo accounts are usually set by the issuer, not the user (e.g., credentials may be “NamedUser-Demo” with a password of “demo”) are can often be easily guessed. <http://www.webfilesys.de/webfilesys-home/onlineDemo.html>. In the case of Mr. Burke, however, the entity to which the demo credential was issued published their userid and password publicly on their own website.

“in the clear.” Anyone with the right web address can view them. Access requires no special equipment, no special tools, and no userid or password. In short, Mr. Burke engaged in journalism. He simply collected and reported on newsworthy content in the public domain on the internet.

On May 9, 2023, federal agents, armed with a search warrant, carried out the unprecedented seizure of the entirety of Mr. Burke’s newsroom, which included his entire office, work product, source material, identity of sources, unpublished materials and publishing equipment- seizing more than 100 Tb of data and the hardware in which it was held (inventory, **Exhibit A**).⁵ For more than two months, counsel has since been engaged in efforts to effectuate the return of Mr. Burke’s property, and as evidenced by the July 17, 2023 letter from attorney Mark Rasch to AUSA Jay Trezevant, (**Exhibit B**)⁶. The government has agreed to return and not retain copies of the hard drives which contain no data related to Mr.

⁵ Garcia, Justin, Tampa City Council member Lynn Hurtak’s home searched by FBI: Hurtak’s husband, Tim Burke, said that it was his name on the search warrant., Tampa Bay Times, May 9, 2023, <https://www.tampabay.com/news/florida-politics/2023/05/08/tampa-city-council-member-lynn-hurtaks-home-searched-by-fbi/> (last visited May 10, 2023).

⁶ The government disputes some of the assertions in the letter, and we accept as accurate the government’s version. The government disputes the opening assertion that the USAO in Tampa is having its communications “regularly reviewed” by Main Justice (Exhibit B, p. 1, par. 1) but clarifies that “there are a number of issues and DOJ policies that require review at different levels.” Similarly, we did not mean to suggest that the USAO was not taking the matter seriously when we noted that this case was not a “priority” (Exhibit B, p. 15, par 2) and believe that the AUSA is working diligently and in good faith -- particularly in efforts to return materials that are not covered by the warrant, none of which have yet been returned. Additionally, by way of clarification, the requirement that Mr. Burke waive his Fifth Amendment rights (Exhibit B, p.2, par. 2) is not a precondition of his access to the cell phone and the MFA, but rather was intended to speed the process of cloning the phone - with the FBI and CART team insisting on making the forensic mirror before permitting Mr. Burke to retrieve his MFA credentials.

Burke's access to and publication of live feeds after August of 2022 - the period mentioned in Attachment B of the Warrant. ⁷ In short, the government has agreed to return -- over more time -- materials that were never covered by the warrant, some of which include journalistic work product, sources and methods, privileged communications, and related materials. They have not agreed to provide copies of his work product, including the thousands of live feeds which make up the privileged contents of Mr. Burke's newsroom.

As a result of the seizure, Mr. Burke has ceased publication, cannot access his investigative materials, and cannot access his social media accounts which are locked by MultiFactor Authentication (MFA) uniquely tied to the seized items. ⁸ The search of a journalist for records related to protected newsgathering, and the seizure and retention of these materials cause irreparable harm, and entitle Mr. Burke to relief under Rule 41(g) F.R. Crim. P. for immediate return of the seized items, materials, information, and all forensic copies made by the government.

⁷ The government has also agreed to provide copies of the portions of drives which contain both materials covered and not covered by the Warrant Attachment, but with those materials covered by the warrant deleted, and with the government retaining the original drives containing the mixed materials. Finally, the government has indicated that it wishes Mr. Burke to provide his Personal Identification Number (PIN) and password to access a seized cell phone in order to facilitate the government's cloning of the phone as a precondition for permitting him to access the phone (or its clone) to recover keys to access his social media accounts. Mr. Burke has been locked out of these accounts since the raid.

⁸ On July 21, 2023, Mr. Burke was permitted to visit the offices of the FBI in Tampa and have limited access to the cell phone containing the credentials necessary for MultiFactor Authentication to his Twitter account. We believe that, as of that date, Mr. Burke will be able to access the Twitter account that he had been locked out of for seventy-three days.

II. Background

Timothy Burke is a respected journalist who has reported for many years on matters of public concern. During his reporting career, he has developed a specialization in finding and reporting on information found in streaming live video feeds. He has a well-deserved reputation as a “person who finds things” on the Internet,⁹ just as he did in this instance. For example, his work exposing the hoax behind Notre Dame football player Manti Teo’s fake dead girlfriend made him a finalist for the Newhouse School’s John M. Higgins Award for Best In-Depth/Enterprise Reporting.¹⁰ He appeared in a 2022 Netflix documentary called “Untold: The Girlfriend Who Didn’t Exist,” which recounted his reporting of the Manti Teo’s story and the resulting scandal.¹¹ His video about Sinclair Broadcast Group’s “extremely dangerous to our democracy “ fake news screed earned him a National Magazine Award nod.¹² Since leaving his role as Director of Video Journalism for The Daily Beast,¹³ he has worked as a freelance journalist

⁹Jack McCordick, FBI Raid of Tampa Journalist Connected to Tucker Carlson Leaked Clips, Vanity Fair, May 27, 2023, available at <https://www.vanityfair.com/news/2023/05/tucker-carlson-leaks-fbi-investigation-tampa-journalist> noting that Burke “was known for having “a reputation as somebody who finds things.”

¹⁰ Wendy S. Loughlin, Newhouse Announces Finalists in 2014 Mirror Awards Competition, Syracuse University News, April 1, 2014, <https://news.syr.edu/blog/2014/04/01/newhouse-announces-finalists-in-2014-mirror-awards-competition-87268/>

¹¹ Untold: The Girlfriend Who Didn’t Exist, Ryan Duffy and Tony Vainuku, Player’s Tribune Production Company, 2022 Netflix series.

¹² Emily Stewart, Watch: dozens of local TV anchors read the same anti-“false news” script in unison. Dozens of anchors. Same Sinclair script., Vox News, April 2, 2018, available at <https://www.vox.com/policy-and-politics/2018/4/2/17189302/sinclair-broadcast-fake-news-biased-trump-viral-video>

¹³ Rachel Olding, FBI Raid on Journo’s Home Reportedly Related to Embarrassing Tucker Carlson

contributing to publications both national and local. His work is also regularly featured on both traditional cable news channels and programs such as *Last Week Tonight with John Oliver* and *The Daily Show*. Some of his investigative projects are published under his own byline, and for others, he is contracted by news organizations and other reporters to contribute his specific set of digital newsgathering and investigative reporting skills. Most recently, he published a video of Oakland A's announcer Glen Kuiper appearing to use a racial slur on-air during a broadcast--an act that, after more than 15 million people viewed Mr. Burke's video, led to Kuiper's firing.¹⁴

Mr. Burke also works as a digital media consultant, helping to launch news start-ups and training journalists with his unique skills of online newsgathering and reporting. The tools he's developed and shared with reporting partners have produced some of the most-seen viral news videos of all time. His media clients rely on the tools he has built, which exist solely in the hardware and backup drives currently in the possession of the FBI. He has been unable to report news or service his clients' reporting since the search warrant was executed; both his journalism career and his business have been brought to a complete standstill and he is unable to earn a living, as his career and his reporting are inseparable from the hardware and intellectual property seized by the government. Moreover, the seizure of his

Vids, Daily Beast, May. 27, 2023 , available at <https://www.thedailybeast.com/raid-on-journalist-tim-burkes-home-related-to-tucker-carlson-videos-report>

¹⁴ A's announcer Glen Kuiper apologizes for appearing to use racial slur during broadcast, ESPN News Services, May 6, 2023, available at https://www.espn.com/mlb/story/_/id/37504577/a-announcer-glen-kuiper-apologizes-appearing-use-racial-slur-broadcast.

journalistic work product, resources, and hardware has also inhibited the reporting and First Amendment activities of his media clients. He is a “person who finds things” on the Internet. What he is not, however, is a criminal.

III. Standard for Return of Property

“A motion to return seized property under Fed.R.Crim.P. 41(g), is a motion in equity, in which courts will determine all the equitable considerations in order to make a fair and just decision.”¹⁵ When considering an equitable remedy in the course of an ongoing criminal action, the exercise of equitable jurisdiction must be made “with caution and restraint” and only in “exceptional cases where equity demands intervention.”¹⁶ This depends then on the so-called “*Richey*” factors:¹⁷ “(1) whether the government displayed a “callous disregard” for the plaintiff’s constitutional rights; (2) “whether the plaintiff has an individual interest in and need for the material whose return he seeks”;¹⁸(3) “whether the plaintiff would be irreparably injured by denial of the return of the property”; and (4) “whether the

¹⁵ *United States v. Howell*, 425 F. 3d 971, 974 (11th Cir. 2005).

¹⁶ *Trump v. United States*, 54 F. 4th 689 (11th Cir. 2022), citing *In re \$67,470*, 901 F.2d 1540, 1544 (11th Cir., 1990).

¹⁷ *Richey v. Smith*, 515 F.2d 1239, 1243–44 (5th Cir. 1975) Because the Fifth Circuit issued this decision before the close of business on September 30, 1981, it is binding precedent in the Eleventh Circuit. See *Bonner v. City of Prichard*, 661 F.2d 1206, 1209 (11th Cir. 1981) (en banc) cited in *Trump v. United States*, 54 F. 4th 689, 694 (11th Cir., 2022)

¹⁸ A motion to return may be filed by any person “aggrieved by an unlawful search and seizure or by the deprivation of property.” *In re Sealed Search Warrant and Application for a Warrant by Telephone or Other Reliable Electronic Means*, 11 F.4th 1235, 1245-1246 & n.6 (11th Cir. 2021). *Harbor Healthcare System, L.P. v. United States*, 5 F.4th 593, 59 note 2 (5th Cir. 2021). (“When the motion [to return property] is made by a party against whom no criminal charges have been brought, such a motion is in fact a petition that the district court invoke its civil equitable jurisdiction.”) *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1172 (9th Cir. 2010) (en banc), overruled in part on other grounds, *Hamer v. Neighborhood Housing Services of Chicago*, 138 S. Ct. 13, 21, 199 L. Ed. 2d 249 (2017).

plaintiff has an adequate remedy at law for the redress of his grievance." Primary consideration is given to the first of these factors.¹⁹ To file a motion for return of property, the seizure need not have been unlawful.²⁰ Even if the initial seizure were lawful, the court has the equitable power to order the materials to be returned where, as here, the continued retention of these documents is unlawful.²¹

IV. Argument

The government searched for and seized Mr. Burke's Newsroom based on a novel and unsupported interpretation of the CFAA and wiretap laws, without appropriate deference to his status as a journalist in a way that acted as a prior restraint on his speech, and both the search and continued retention of his work product demonstrates a continuing callous disregard for his Constitutional rights under *Richey*.

¹⁹ The "foremost consideration" for a court when deciding whether it may exercise its equitable jurisdiction in this context. *United States v. Chapman*, 559 F.2d 402, 406 (5th Cir. 1977). When considering this factor, our precedent emphasizes the "indispensability of an 'accurate allegation' of 'callous disregard.'" *Id.* (quoting *Richey*, 515 F.2d at 1243); See also *Hunsucker v. Phinney*, 497 F.2d 29, 34 n.10 (5th Cir. 1974).(collecting cases).

²⁰ Amendments to motion to return Rule in 1989 were designed to expand the Rule's coverage to include motions to return property lawfully seized. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1173 (9th Cir. 2010) (en banc), overruled in part on other grounds, *Hamer v. Neighborhood Housing Services of Chicago*, 138 S. Ct. 13, 21, 199 L. Ed. 2d 249 (2017). Regardless of whether initial seizure of property under criminal forfeiture statute was lawful or unlawful, district court had authority under Rule of Criminal Procedure dealing with motions for return of property to address both lawfulness of initial seizure and continued retention of property. *United States v. Schmitz*, 153 F.R.D. 136 (E.D. Wis. 1994).

²¹ The Advisory Committee Note to the 1989 amendment states in part, "The amendment to Rule 41(e) conforms the rule to the practice in most districts and eliminates language that is somewhat confusing." As amended, Rule 41(e) [the precursor of what is now Rule 41(g)] provides that an aggrieved person may seek return of property that has been unlawfully seized, and a person whose property has been lawfully seized may seek return of property when aggrieved by the government's continued possession of it."

A. The Search and Seizure of Mr. Burke’s Newsroom Violated His Rights Under the First and Fourth Amendments, and Displayed A “Callous Disregard” for His Constitutional Rights

The government has engaged in an almost unprecedented search for and seizure of a journalist’s work, including information he collected with the intent to disseminate it to the public. DOJ regulations recognize the harm to the First Amendment resulting from even seeking a warrant to seize a newsroom.²² Similarly, the Privacy Protection Act (“PPA”), 42 USC 2000aa(a), prohibits the government from even seeking a warrant “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...”²³ Search warrants and seizures of reporters, like that in

²² If the proposed warrant creates a “close or novel question” of whether the search involves the journalists’ news gathering activities, the approval of the Deputy Assistant Attorney General for the Criminal Division, is required, and if there is “genuine uncertainty” whether the member of the news media is acting within the scope of newsgathering, the Attorney General must personally approve the seeking of the warrant. 28 CFR 50.10(e)(2) In either case, if the warrant proposes to authorize a search of “the premises of a news media entity,” *the Attorney General must personally approve the application.* 28 C.F.R. 50.10(d)(2)(ii). add "The kinds of cases in which DOJ authorized searches of journalists' computers are usually those in which journalists are alleged to have committed offenses wholly apart from their newsgathering functions, like insider trading, threats, or possession of child pornography. Such a search warrant led to the guilty plea by journalist James Gordon Meek to child pornography charges on July 21, 2023 in the Eastern District of Virginia. See, Salvator Rizzo, Former ABC News Journalist Pleads Guilty in Child Porn Case, The Washington Post, July 21, 2023, available at <https://www.washingtonpost.com/dc-md-va/2023/07/21/james-meek-abc-news-guilty-plea/> (in response to allegations that the search warrant was to look for classified information on Meeks' computer "Such an investigation would raise thorny First Amendment concerns. In 2022, acting on a pledge from President Biden not to seize journalists’ phone or email records, the Justice Department issued formal regulations restricting how federal prosecutors can pursue leak investigations. But the Meek case was never about his reporting, U.S. Attorney Jessica D. Aber said in a statement.")

²³ The statute continues noting an exception to this provision, noting “[t]hat a government officer or employee may not search for or seize such materials under the provisions of this paragraph if the offense to which the materials relate consists of the receipt, possession, communication, or

this case, serve as a prior restraint on publication,²⁴ and fundamentally interfere with First Amendment protected news gathering and reporting.²⁵

Against this principle is the fact that the government is entitled to investigate certain crimes *even if committed by journalists*. But they must actually be crimes - not a pretext to avoid the strictures of the PPA. Thus, the PPA provides that a search warrant may be obtained if “there is probable cause to believe that the person possessing such materials has committed or is committing the criminal offense to which the materials relate” *Id.* Similarly, under 28 C.F.R. 50.10 (b)(1)(ii)(B), “newsgathering does not include criminal acts committed in the course of obtaining information or using information, such as: breaking and entering; theft; unlawfully accessing a computer or computer system; unlawful surveillance or wiretapping; bribery; extortion; fraud; insider trading; or aiding or abetting or conspiring to engage in such criminal activities, with the requisite criminal intent...” These so-called “suspect” exceptions would permit some searches of a journalist (with appropriate AG approvals and restrictions) if there was evidence that the journalist committed criminal acts (other than the receipt of

withholding of such materials or the information contained therein” unless it relates to classified information. *Id.*

²⁴ *Near v. Minnesota*, 283 U.S. 697, 713 (1931).

²⁵ In *Zurcher v. Stanford Daily*, 436 U.S. 547, 566 (1978) the Supreme Court permitted a search warrant to be served on a student newspaper, noting that “There is no reason to believe, for example, that magistrates cannot guard against searches of the type, scope, and intrusiveness that would actually interfere with the timely publication of a newspaper. Nor, if the requirements of specificity and reasonableness are properly applied, policed, and observed, will there be any occasion or opportunity for officers to rummage at large in newspaper files or to intrude into or to deter normal editorial and publication decisions. “

or requesting of information) in the course of newsgathering. With this predicate we examine the seizure in this case.

B. Access To The Sworn Affidavit Is Essential to Determine The Validity of the Application for And Issuance of the Search Warrant.

Mr. Burke is at a disadvantage when seeking the remedy of return of illegally seized property because he is unable to know the justification used by the government to conduct the search. We have requested the sworn affidavit and been rebuffed. We still don't know their theory of the crimes alleged. We don't know what the Magistrate Judge was told about the factual basis of the alleged offenses, whether the Magistrate was even told that Mr. Burke was a journalist, and that the government was seeking privileged information and journalist work product, or whether in seeking the warrant the AUSA followed DOJ policies on seeking *personal approval* by the Attorney General and specification about the protective measures the agents were to use to search seized computers for specific files that represent evidence of crime but which may be intermingled with entirely innocuous information. If the search strategy was influenced by legal considerations such as potential PPA liability, the affiant should explain how they are to protect First Amendment materials.²⁶ Similarly, we don't know if the affiant or the Magistrate provided a post-seizure strategy to the searching agents to avoid contact with First Amendment or otherwise privileged information, or required

²⁶ Computer Crime And Intellectual Property Section (CCIPS) Guide to Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, January 2001, available at <http://neiassociates.org/ccips/> at II(2).

any special minimization procedures as provided by the DOJ Computer Crime and Intellectual Property Section for searches involving privileged or PPA-protected information, or if they mandated the appointment of a Special Master or a “taint team.” Although none of these protective procedures would make this search lawful, we simply have no information on whether they were or were not imposed or followed.

Other news media – most notably the Tampa Bay Times -- have unsuccessfully sought access to the affidavit in support of this warrant on First Amendment right of access to public records grounds.²⁷ We adopt and incorporate their arguments, as well as the argument that the government’s opposition to unsealing the affidavit is based only on vague and unsupported allegations of unspecified potential harm.²⁸

Mr. Burke has a higher interest in disclosure of the affidavit. It was his materials seized, and his access to the affidavit is essential to challenge whether the government even was permitted to seek, much less the Magistrate had authority to issue, this warrant.²⁹ Indeed, when the subject of the investigation

²⁷ *Times Publishing Co., Inc., v. United States*, Case No.: 8:23-mc-00014-WFJ-SPF (M.D. Fl., 2023)Dkt. Entry. 1, p. 3.

²⁸ *Id.*, Dkt. Entry 22, p. 3-6

²⁹ The Eleventh Circuit does not seem to have opined on the question of whether the subject of an investigation has a right, either under the common law, the Fourth Amendment, or Rule 41 F.R.Crim.P. to access to an affidavit in support of a warrant in order to challenge the lawfulness of the warrant, but multiple other courts have found such a right. See, *Societe d'Equipments Internationaux Nigeria, Ltd. v. Dolarian Capital, Inc.*, No. 15-cv-1553-DAD-SKO, 2016 WL 4191887, at **1-2 (E.D. Cal. Aug. 8, 2016; *In re Offs. & Storage Areas Utilized by Stephen P. Amato, D.C., P.C.*, No. 05-MJ-05-B, 2005 U.S. Dist. LEXIS 6870, at **16-23 (D. Me. Apr. 14, 2005) (holding that Fourth Amendment right that warrants not issue except upon probable cause “implies a right, in a person

seeks access to this information in order to challenge the lawfulness of the search and seizure, the balance tips in favor of disclosure. As the Court held in *Matter of Up North Plastics, Inc.*, 940 F. Supp. 229 (D. Minn., 1996) concerns about privacy and general access to sealed affidavits *to the public* do not implicate the rights of a *person who has been subject to a search warrant*. In fact, “a person whose property has been seized pursuant to a search warrant has a right under the warrant clause of the Fourth Amendment to inspect and copy the affidavit upon which the warrant was issued, and the court can delay the exercise of that right only upon a showing of a compelling governmental interest that cannot be accommodated by some means less restrictive than sealing the court's records.”

whose property has been subjected to search and/or seizure pursuant to a warrant, to challenge whether the warrant was in fact predicated on probable cause,” which “in turn, implies a right to view the underlying materials that purportedly established probable cause for the search”) (citations omitted); *In re Search Warrants Issued on April 26, 2004*, 353 F.Supp.2d 584, 587-91 (D. Md. 2004) (affirming magistrate judge's determination that Fourth Amendment confers pre-indictment right of access to redacted search warrant affidavit on target of search, where government failed to demonstrate compelling governmental interest in keeping affidavit sealed); *In re Search Warrants Issued on Aug. 29, 1994*, 889 F.Supp. 296, 299 (S.D. Ohio 1995) (Fourth Amendment right to be free of unreasonable searches and seizures includes right to examine the search warrant affidavit after the search has been conducted, absent government showing of compelling governmental interest and the unavailability of less restrictive means, such as redaction); *In The Matter Of Amato*, Docket No. 05-MJ-05-B. (D. Maine 2005); *United States v. Oliver*, No. 99-4231, 2000 WL 263954, at **2 (4th Cir. Mar. 9, 2000) (such a right exists); *Sloan v. Sprouse*, 968 P.2d 1254, 1258 (Okla. Crim. App. 1998) (same); Other courts have not found such a right. *Matter Of The Search Of The Scranton Housing*, 436 F. Supp. 2d 714, 723 (MD Penn., 2006); *In re Grand Jury Proceedings*, 115 F.3d 1240, 1246 (5th Cir.1997); *In re EyeCare Physicians of Am.*, 100 F.3d 514, 517 (7th Cir.1996); *In the Matter of the Search of Flower Aviation of Kansas, Inc.*, 789 F.Supp. 366, 369 (D.Kan.1992)(“movant has not challenged the lawfulness of the search in the manner in which it was executed, nor has the movant challenged the scope of the warrant.”); *Bennett v. United States*, No. 12-61499-CIV, 2013 WL 3821625, at *4 (S.D. Fla. July 23, 2013) (J. Rosenbaum). *Lindell v. United States*, 22-cv-2290 (ECT/ECW) (D. Minn. Nov. 3, 2022).

Likewise, in *In re Extradition of Manrique*, Case No. 19-mj-71055-MAG-l (TSH), 12-13 (N.D. Cal. Feb. 6, 2020) the District Court noted that, “[t]o permit an affidavit or any documents in support of a search warrant to remain sealed against examination by the person whose property was searched deprives him of the right secured by Rule 41 to challenge that search. There is nothing in Rule 41 to suggest that such evidence is intended to be taken in secret or without a full opportunity for the aggrieved person to argue that probable cause was lacking.” Even if secrecy could be justified to keep the warrant affidavit from the press generally, where, as here, the government has no evidence that Mr. Burke will destroy evidence, threaten witnesses, or otherwise obstruct their investigation, there is no reason to keep him from learning why his own newsroom and work product was seized. Where access to the affidavit is essential for him to challenge the lawfulness of the search under Rule 41(g) F.R. Crim. P. and under *Franks v. Delaware*, 438 U.S. 154, 156, 165-71 (1978), it must be disclosed.³⁰

C. There Was No Crime. The CFAA & Electronic Communications Act Cannot Be Read To Criminalize Routine Newsgathering from the Internet

The government is permitted to seek a warrant to seize a newsroom only if it is not a “close question” of whether a crime occurred. Here, the government seeks to make the process of searching, finding, scraping, and indexing live feeds on the

³⁰ If the Court does not wish to make the affidavit public, the Court could provide a copy thereof to Mr. Burke and/or his counsel under seal, with directions that any subsequent filings referencing the affidavit similarly be either redacted in part or filed under seal, if the Court is convinced by the government’s arguments that release of the affidavit will result in harm to witnesses and possible flight of suspects.

public Internet into a crime. It appears to do so through a fundamental misreading of the provisions of the CFAA, apparently interpreting “unauthorized access” as “access not expressly granted.” That is not what the statute says. The relevant language of 18 USC 1030(a)(2)(c) makes it a crime to “intentionally access[] a computer without authorization or exceeds authorized access, and thereby obtain[] ...information from any protected computer.”³¹ As the Supreme Court noted just this term in *Dubin v. United States*,³² “[c]rimes are supposed to be defined by the legislature, not by clever prosecutors riffing on equivocal language.” The Supreme Court also noted that, with specific regard to the ambiguous terms in the CFAA, “this Court has prudently avoided reading incongruous breadth into opaque language in criminal statutes.”³³ The term “without authorization” cannot be read to mean “in a way that the owner did not want” or “for a purpose unintended by the owner.” To read the criminal hacking statute so broadly would prohibit many forms of journalism, as the purpose of investigative journalism is to find and report on things that persons or entities, including powerful entities like Fox News, may not wish disclosed.

When Congress prohibited “access[ing] a computer without authorization,” (18 U.S.C. § 1030(a)), it intended to prohibit conduct “analogous to . . . ‘breaking

³¹ For the purposes of this motion, we do not contest that the website Mr. Burke accessed is a “protected computer,” or that the list of URL’s obtained by accessing that website is “information.”

³² Dkt. No. 22-10, June 8, 2023, Slip Op., 17-18 (citation omitted).

³³ *Id.*, citing *Van Buren v. United States*, 593 U.S. ____, 141 S. Ct. 1648, 1661(2021)(“the Government’s interpretation of the [CFAA] statute would attach criminal penalties to a breathtaking amount of commonplace computer activity.”)

and entering,”³⁴ That is, it prohibited “hacking.”³⁵ As an “anti-hacking” statute, the criminal provisions of the CFAA have been read narrowly, consistent with due process limitations on expansive reading of criminal statutes.³⁶ This is true where, as here, the broad statutory interpretations suggested by the government risk

³⁴ H.R.Rep. No. 98-894, 2d Sess., p. 20 (1984); *US v. Nosal*, 676 F.3d 854, 857 (9th Cir., 2012) (“The government’s interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute.”); *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 932 (E.D. Va., 2010) (“The CFAA is a civil and criminal anti-hacking statute designed to prohibit the use of hacking techniques to gain unauthorized access to electronic data.”); *Fidlar Technologies v. LPS Real Estate Data Sols.*, 810 F.3d 1075, 1079 (7th Cir., 2016) (“The CFAA, 18 U.S.C. § 1030, is primarily a criminal anti-hacking statute.”); *Andrews v. Sirius XM Radio Inc.*, 932 F.3d 1253, 1263 (9th Cir., 2019) (“the CFAA is ‘an anti-hacking statute,’ not ‘an expansive misappropriation statute.’”) citing (*Nosal I*) (en banc); *United States v. Aleynikov*, 737 F. Supp. 2d 173, 192 (S.D.N.Y., 2010) (“This interpretation of § 1030(a)(2)(C) comports not only with the plain meaning of the statutory text, but also with the overall structure and purpose of the CFAA.”)

³⁵ *hiQ Labs I*, *supra*, 938 F.3d at p. 1000; see also, e.g., *United States v. Thomas* (5th Cir. 2017) 877 F.3d 591, 596 (noting the statute has an “anti hacking purpose”)

³⁶ Due process requires that criminal statutes provide ample notice of what conduct is prohibited. *Connally v. Gen. Const. Co.*, 269 U.S. 385, 390 (1926). Vague laws that do not “provide explicit standards for those who apply them . . . impermissibly delegate[] basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis.” *Grayned v. Rockford*, 408 U.S. 104, 108-09 (1972). A criminal statute that fails to provide fair notice of what is criminal—or threatens arbitrary and discriminatory enforcement—is thus void for vagueness. *Skilling v. United States*, 561 U.S. 358, 412 (2010) (citing *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). As a result, in attempting to interpret the provisions of a statute -- particularly a criminal statute like the CFAA, to attempt to punish conduct which is protected by both due process and the First Amendment, Courts traditionally interpret the statute narrowly in favor of the accused. *United States v. Santos*, 553 U.S. 507, 514 (2008). The Supreme Court noted that this “ensures fair warning by so resolving ambiguity in a criminal statute as to apply [] only to conduct clearly covered.” *United States v. Lanier*, 520 U.S. 259, 266 (1997). As the Ninth Circuit explained in analyzing the ambiguous “access without authorization” provisions of the CFAA, this approach “not only ensures that citizens will have fair notice of the criminal laws, but also that [a legislature] will have fair notice of what conduct its laws criminalize. We construe criminal statutes narrowly so that [a legislature] will not unintentionally turn ordinary citizens into criminals.” *Nosal I*, 676 F.3d at 863.; cf. *Sandvig*, 451 F. Supp. 3d at 88 (suggesting that the CFAA must be narrowly applied to “hacking” situations) Defining the term “access without authorization” should not be left to the vagaries of individual prosecutors to determine what kinds of conduct “are so morally reprehensible that they should be punished as crimes[.]” See *United States v. Kozminski*, 487 U.S. 931, 949 (1988). Doing so merely “invited discriminatory and arbitrary enforcement,” of the CFAA See *Nosal I*, 676 F.3d at 862. The Constitution, however, “does not leave us at the mercy of noblesse oblige” by the government. *United States v. Stevens*, 559 U.S. 460, 480 (2010).

violating Mr. Burke's First Amendment rights of speech and of the press and his Due Process rights.³⁷

While we don't fully know the government's theory of the "crime" without access to the affidavit, it appears that the government would assert that Mr. Burke "should have known" that the owners of the live streams did not want him to view their publicly accessible data, and that the fact that the live streams were accessible at "non-obvious" URL's should have put Mr. Burke on notice that these sites did not "authorize" his capture of the live streams.³⁸ This is based on a fundamental misunderstanding of ordinary norms of Internet use.³⁹ It is perfectly normal for internet users to access streaming content in precisely the manner Mr. Burke did. Indeed, simple web searches for m3u8 files will bring up hundreds of such streams

³⁷ Courts have relied upon the canon of constitutional avoidance to narrowly interpret the CFAA in order to avoid creating significant risks to individuals' First Amendment and Due Process rights. See *Sandoig v. Barr*, 451 F. Supp. 3d 73, 88–89 (D.D.C. 2020), appeal docketed, No. 20-5153 (D.C. Cir. May 28, 2020) ("Plaintiffs' First Amendment challenge raises such risks . . . and thus weighs in favor of a narrow interpretation under the avoidance canon." Holding the CFAA does not criminalize mere terms-of-service violations on consumer websites.); *Nosal I*, 676 F.3d at 863 (construing the CFAA narrowly "so that Congress will not unintentionally turn ordinary citizens into criminals"). The Supreme Court has recognized that "state action to punish the publication of truthful information seldom can satisfy constitutional standards." *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 102 (1979).

³⁸ With respect to Mr. Burke's use of the public credential to access "Website-1," the government may argue that the use of the shared demo credential was not explicit authorization, and again that Mr. Burke "should have known" that the public sharing by the account owner of the credential did not "authorize" the use of the shared credential. Such an interpretation -- that password sharing is a crime -- would create criminal liability to the more than 100 Million Netflix users who routinely share their own passwords. Todd Spangler, *Netflix Estimates More Than 100 Million Non-Paying Households Use Shared Passwords*, *Variety*, Apr 19, 2022 available at <https://variety.com/2022/digital/news/netflix-sharing-password-100-million-1235236051/>

³⁹ Cf. Kerr, *Norms of Computer Trespass* (2016) 116 *Colum. L.Rev.* 1143, 1162 ("The first step in applying computer trespass law to the Web is to identify the nature of the space that the Web creates).

-- accessible simply by either clicking a link or putting a URL into a browser window.

Moreover, even actual notice that a website owner does not appreciate a user's access is not enough to trigger liability for "unauthorized access" under the CFAA, and the government's theories to the contrary highlight the pitfalls of adopting such an approach. (See, *hiQ Labs I*, 938 F.3d at pp. 1001–02, *Sandvig v. Barr*, 451 F. Supp. 3d at pp 88-89) It is wholly unreasonable to expect a journalist who finds information or streaming content on a publicly accessible website to assume that the person or persons who put the content out there in the public domain "did not know" or "did not want" that content to be publicly accessible simply because the URL is "non-obvious." ⁴⁰ See, *United States v. Morel*, 922 F.3d 1, 10–11 & fn. 9 (1st Cir. 2019)(defendant had no reasonable expectation of privacy in images hosted at a URL "composed of random numbers and letters" because the URL was nevertheless accessible to anyone who stumbled across it.) This is for good reason: It is difficult, if not impossible, for a user to know if a URL is "non obvious" from the website owner's perspective. Visitors to a specific URL have no way of knowing in the abstract if unencrypted unprotected content was "private" and access to it was intended to be "unauthorized."

Further, the government's theory that Mr. Burke, by accessing publicly addressable URL's containing live streams also violated the wiretap law by

⁴⁰ Kerr, *supra*, 116 Colum. L.Rev. at pp. 1164– 65 "A hard-to-guess URL is still a URL, and the information posted at that address is still posted and accessible to the world"

“intercepting” (acquiring the contents of) “private” communications is similarly precluded by the language of the statute itself which expressly permits access to an “electronic communication system that is configured so that such electronic communication is readily accessible to the general public.” 18 U.S.C. § 2511(2)(g). *Snow v. DirecTV, Inc.*, 450 F. 3d 1314, 1320-21 (11th Cir., 2006). All of this should have been told to the Magistrate when seeking a warrant based on this theory of criminal liability. We suspect that it was not.

Without a violation of the CFAA or a violation of the wiretap laws, there is no legal justification for the application for the warrant -- and indeed, even petitioning the Magistrate for the warrant violates the PPA and DOJ policy. This demonstrates “callous disregard” for Mr. Burke’s rights under *Richey*. Even if Fox News didn’t want Mr. Burke to report on what it had made public, and even if entities did not know they were publicly streaming their live feeds, the fact of the matter is that they were, and that they are. Accessing and collecting these feeds from public sources is simply not a crime.

D. The Execution of the Search and the Retention of the Seized Items Is An Unconstitutional “Prior Restraint” On Mr. Burke’s Rights Under the First Amendment.

Mr. Burke suffers irreparable harm by the government’s seizure of and retention of his newsroom. Taking his computers, his data, his notes, his entire newsroom, and refusing to return them is the ultimate “prior restraint” on his free speech. He cannot “publish” because he cannot access either his data, his work product, his social media accounts, or his equipment with which to publish. He

cannot distribute newsworthy information because the government has taken this information. The “chief purpose” of the First Amendment is to prevent “previous restraints upon publication.” *Near v. Minnesota*, 283 U.S. 697, 713 (1931); see also *Se. Promotions, Ltd. v. Conrad*, 420 U.S. 546, 553 (1975) (“Our distaste for censorship—reflecting the natural distaste of a free people—is deep-written in our law.”). Prior restraints are the “most serious and the least tolerable infringement on First Amendment rights” because they are “an immediate and irreversible sanction,” not only “chill[ing]” speech but also “freez[ing]” it, at least for a time. *Nebraska Press Ass’n*, 427 U.S. at 559. And there is a “heavy presumption against [the] constitutional validity” of a prior restraint under federal constitutional law. Prior restraints are “disfavored in this nation nearly to the point of extinction,” *United States v. Brown*, 250 F.3d 907, 915 (5th Cir. 2001).

Not only is the seizure and continued possession of Mr. Burke’s materials a prior restraint, it also imposes a “chilling effect” on Mr. Burke, his media clients and other journalists’ future reporting. The government’s seizure of information about Mr. Burke’s sources and methods, who provides him information and who he provides information to, and other materials protected under the Florida journalist shield law causes irreparable harm to Mr. Burke, his sources, and the other journalists with whom he works. ⁴¹

⁴¹ In other cases where the government has seized, or attempted to seize records of journalists who accessed and reported on public information alleging that such access was unauthorized,” courts have routinely rejected the government’s assertions. See, e.g., *City of Fullerton v. Friends for Fullerton’s Future, et al.*, Orange County Superior Court Case No. 30-20\9-01107063-CU-NP-CJC. (government paid legal fees and expenses and returned documents to civic group

As noted, searches and seizures from journalists are extraordinary events. Since the landmark Supreme Court case of *Zurcher v. Stanford Daily*, 436 U.S. 547, 98 S.Ct. 1970 (1978) there have only been a handful of search warrants issued against journalists for information concerning their news gathering efforts. In fact, both Congress,⁴² the Department of Justice,⁴³ and the Florida legislature⁴⁴ passed laws and promulgated regulations designed to make it *presumptively unlawful for DOJ employees to seek warrants to obtain precisely the kind of materials from a journalist as were seized from Mr. Burke here.*

accessing City website and obtaining documents they were allegedly not supposed to have after seizure of documents and criminal investigation of group for “hacking”); John Leyden, Police probe Schwarzenegger audio 'hack' Sex, lies and audio-files, September 13, 2006, available at https://www.theregister.com/2006/09/13/schwarzenegger_audio_hack/; In the Matter of Brian Carmody, Dkt. No. 2516765 (Cal. Sup. Ct., County of San Francisco, August 2, 2019)(government’s failure to inform issuing magistrate of status of subject of search warrant as journalist invalidated warrant). Issie Lapowsky, Shadow Politics: Meet the Digital Sleuth Exposing Fake News, Wired Magazine, July 18, 2018 available at <https://www.wired.com/story/shadow-politics-meet-the-digital-sleuth-exposing-fake-news/> (discussing the use by journalist Jonathan Albright of the CrowdTangle tool to access Facebook sites using an API and obtain information about Russian interference with the 2016 election.

⁴² The Privacy Protection Act, 42 USC 2000aa(a)

⁴³ CFR 50.10 (a)(1); Final Rule Approved by AG Garland October 26, 2022, Docket No. OAG 179; AG Order No. 5524-2022, available at

https://www.justice.gov/d9/pages/attachments/2022/10/26/ag_order_5524-2022_media_policy_20221026.pdf; United States Attorney’s Manual 9-13.400; Memorandum of Attorney General Garland, Use of Compulsory Process to Obtain Information From, Or Records Of, Members of the News Media, July 19, 2021 (“the Garland Memo”) available at <https://www.justice.gov/ag/page/file/1413001/download>; Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations Computer Crime and Intellectual Property Section Criminal Division Published by Office of Legal Education Executive Office for United States Attorneys, available at <https://www.justice.gov/file/442111/download>

⁴⁴ Fl. Stat. 90.5015, applicable in federal court under F.R.E. 501, see, *Riley v. City of Chester*, 612 F.2d 708, 713-16 (3d Cir. 1979)(recognizing a federal common law journalist privilege);


V. Conferral

The assigned Assistant United States Attorney, Jay Trezevant, Esquire, opposes the Motion to Unseal and for Return of Property under Rule 41g.

VI. Conclusion

Mr. Burke embarrassed Fox News by broadcasting that which they would have preferred not to have broadcast. He has similarly embarrassed other entities by providing copies of live streaming video to other news outlets for publication. In every case, this publicly accessible content was found through his diligence, perseverance, intelligence, and insight. It was not found through “hacking.” The data he found was public, internet-addressable, non-encrypted, unprotected internet content. If the sworn affidavit avers something else, this would be news to us. If the government urges that publication of embarrassing stories like the Carlson/Ye broadcast requires the express consent of Fox News, they are wrong. Such an assertion is novel, unsupported by the law, and inconsistent with the First Amendment. Mr. Burke therefore seeks an order of this court returning all seized materials and all copies thereof, as privileged and protected under the First Amendment, and an order providing a copy of the sworn affidavit in support of the warrant to Mr. Burke and his counsel.

Respectfully submitted,



Michael P. Maddux, Esquire

Florida Bar # 964212

Michael P. Maddux, P.A.

2102 West Cleveland Street

Tampa, Florida 33606

Email: mmaddux@madduxattorneys.com

Phone: (813) 253-3363

Fax: (813) 253-2553



Mark D. Rasch

Law Office of Mark Rasch

Member, MD, MA, NY Bar

MDRasch@gmail.com

(301) 547-6925

Pro hac vice pending

CERTIFICATE OF SERVICE

I hereby certify that on **July 21, 2023**, a true and correct copy of the foregoing document is being electronically filed and will be furnished via CM/ECF to: Jay Trezevant, Esquire, U.S. Attorney's Office Middle District of Florida, Tampa Division, 400 North Tampa Street, Suite 3200, Tampa, FL 33602 at jay.trezevant@usdoj.gov.



Michael P. Maddux, Esquire