MARK D. RASCH
LAW OFFICE OF MARK D. RASCH
7919 SPRINGER ROAD
BETHESDA, MARYLAND 20817
EMAIL: MDRASCH@GMAIL.COM
TEL: (301) 547-6925
Admitted: NY, MA, MD

July 17, 2023

AUSA Jay Trezevant
United States Attorney's Office
Middle District of Florida
400 N Tampa St
Tampa, Florida 33602

BY EMAIL: Jay.Trezevant@usdoj.gov

Dear Jay:

This will summarize our conversation Friday, and attempt to work out a way forward in this investigation. In that conversation, you indicated that, due to the sensitivity of a criminal investigation of a reporter for activities which presumptively come under the protections of both the First Amendment, the Privacy Protection Act, and DOJ regulations and guidelines on compulsory process to reporters, all of our communication with your office is regularly reviewed by appropriate officials at Main Justice in Washington, D.C. It is for this reason that I seek to explain in some detail why this investigation is unwarranted, unsupported, and in conflict withthe principles of a free press. As far as we can see, they are predicated on an incorrect narrative that Mr. Burke committed some offense, and therefore forfeited his rights as a journalist. He did not. He accessed no computers without authorization, and intercepted no private communications. He engaged in acts and works of journalism. We have been patient in attempting to resolve this matter, but, as I indicated to you, we expect to file a Motion for Return of ALL of Mr. Burke's seized property as having been seized without legal support and in violation of law, policy, regulation and the Constitution.

I. Procedural Matters

With that note, I want to first address some of the non-substantive matters we talked about on Friday. We do appreciate your office's desire to return to Mr. Burke those items that are wholly irrelevant to your investigation of his reporting and publishing practices - items we posit could

not properly have been seized under the warrant (except to the extent that they were on a shared drive with materials covered by the warrant).

A. The Cell Phone/Access to Social Media Accounts

We both agree that, after more than 72 days, it is critical that Mr. Burke be able to access the seized cell phone and restore the Multifactor Authentication necessary for him to access his social media accounts and to do business. You have indicated that you are working with the FBI CART team to enable a process that will permit such access without making unnecessary changes to the forensics of the phone and would provide a stipulation regarding chain of custody issues. (As of this writing we have received and are reviewing the stipulation.)

It does not appear that the process you contemplate would be workable. First, you insist that Mr. Burke waive his Fifth Amendment rights, and provide the agents the passcode necessary to unlock the cell phone [1] to assist agents in cloning his phone as a condition precedent to Mr. Burke having access to either the original or cloned device. Mr. Burke declines to waive his Constitutional right against self-incrimination. Moreover, you have indicated your concern that the mere booting up of the cell phone (taking it out of "airplane" mode) would cause the phone to sync with cloud-based storage services and result in the deletion or alteration of data on the cell phone. Finally, we would have to work out language (you are drafting) to stipulate that, with respect to any of the data to which we are given access, any changes resulting from our access to the data or devices are not forensically significant and does not affect the admissibility of data under F.R.E. 801 and related provisions. In that regard, we have received and are reviewing your proposed stipulation as to authenticity.

B. Drives and Data Outside the Scope of the Warrant

We both agree that drives and devices that only contain materials that are outside the scope of the Warrant and the attachments thereto should be returned without a copy maintained by the government. This includes drives which contain data that is temporally outside the time-frame specified in the warrant, and drives and devices which do not relate to the offenses specified in the warrant (18 USC 1030, 18 USC 2511). Again, as we have emphasized, the designation of drives as being "outside the scope" of the warrant should not be taken as an admission that any data or remaining drives are, in fact "within the scope" of the warrant. As you know, it remains our position that there was no violation of any law, and therefore no "evidence of violation" of any statutes. We have provided you with an initial list of such drives. You have indicated that you intend to return such data (and not retain any copies) beginning next week. We will provide

[1] *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011* (Grand Jury Subpoena), 670 F.3d 1335, 1341 (11th Cir. 2012) ("Here, the Government appears to concede, as it should, that the decryption and production are compelled and incriminatory.").

you with two one terabyte drives to facilitate this process. We may supplement our designation as we learn more about the drives and data seized. In particular, in addition to requesting return of drives, we may add specific DEVICES seized to our list of items to be returned.

C. Drives and Data Which Contain Information You Contend ARE Within the Scope of the Warrant.

With respect to drives, devices or data which contain information you contend are within the scope of the warrant, we agree that such drives and devices are hybrid in nature and contain substantial amounts of information and data which are not covered by the warrant. As a mixed device, the warrant may authorize the seizure of the entire drive, but only authorizes the subsequent search of information which is within the scope of the probable cause determination. We suspect that the magistrate was provided with a procedure to be followed to provide the constitutionally required minimization procedures necessary to ensure that the searches of the drives the magistrate authorized to be seized were conducted in a way that "specifies the place to be searched and the items to be seized" from those drives.

One of the key reasons we continue to seek access to the Affidavit in support of the warrant is to see the minimization procedures that the government proposed to the magistrate, or the minimization procedures adopted by the magistrate by implication. In addition, we presume that these minimization procedures included the mandatory use of either a Special Master or an independent "taint team" to prevent the investigators from being exposed to journalist privileged and First Amendment protected information.

Thus, these drives contain three types of data. Data outside the scope of the warrant (that have nothing to do with the electronic data collection practices of Mr. Burke which you contend were "unauthorized"). You have agreed to provide cloned or copied drives to Mr. Burke which contain this data, and Mr. Maddux will provide a "rolling supply" of 1 Tb drives (or larger) onto which the FBI or CART team will copy this data. Second, the drives contain data which you contend are relevant to the investigation and are covered by the warrant. Within this class of data there is both the data and communications that you contend are relevant to the investigation (e.g., Burke's communications with Twitter sources, information about HOW Mr. Burke accessed publicly accessible streaming video content) and the stored streaming content access itself. For this information, you decline to provide copies of the data to Mr. Burke at this time. Thus, you agree only to provide Mr. Burke with copies of data that is wholly irrelevant to your investigation. Third, there is data which is covered by the terms of the warrant and which is confidential, privileged, or otherwise protected from disclosure to the government. I will address the latter two separately.

D. Attorney-Client and Similar Privileges

You have asked us to designate whether there is any information in any of the seized materials which we contend are protected under privileges other than journalist privileges like attorney/client, doctor/patient, priest/penitent privileges, as well as information like medical records protected under HIPAA and similar laws. We note parenthetically that all such data by definition is outside the scope of the warrant and its attachments. Additionally, we note the difficulty of defining data on drives to which we do not have access. Therefore, our failure to designate a specific file as "privileged" at this time should not be taken as a waiver of our right to later name files or data as privileged at a later date. Additionally, we are talking here ONLY of privileges unrelated to Mr. Burke's journalistic activities. As we discussed, we decline to provide you the names of Mr. Burke's sources for reporting, as providing these names would itself be inconsistent with the assertion of the Florida journalist privilege.

On the seized devices, there are numerous files and communications which contain or are related to either attorney client privileged communications or other federally recognized privileges. I should note in this regard that there is the "dual privilege" problem with respect to Mr. Burke's communications with counsel about matters related to his journalistic endeavors. While the attorney-client privilege traditionally does not extend to the identity of the client (in this case, the other way around with Mr. Burke being the client) or the existence of the relationship, the journalist privilege recognized in Florida extends to the identity of the journalists' sources and methods. Thus, when a journalist seeks counsel, the fact that the journalist is seeking counsel, and the timing of that representation, and the nature of that counsel's specialization can be used to determine the identity and subject matter of the journalists' legal issues and the identity of their privileged sources.

Without waiving either Mr. Burke's attorney-client privilege or his reporters' privilege, we assert privilege with respect to communications with attorneys Sharon L. Levine and Dipesh Patel, as well as attorneys from Levine Sullivan Koch & Schulz, LLP, including but not limited to Thomas B. Kelley, Chad R. Bowman, and Elizabeth Seidlin-Bernstein, as well as internal communications with his former in-house attorney Courtenay O'Connor.

We also note that the seized materials include materials protected from disclosure under Fl. Stat. 455.241(2) and 45 CFR Part 160 and Subparts A and E of Part 164, but we are unable to specifically designate these materials without access to the computers which house this material.

Finally, we also note that there may be materials the seizure of which trigger a legal obligation by Mr. Burke to provide notice to affected individuals under Fl. Stat. 501.171. Again, we cannot designate such information without access to the data seized.

E Data of Ms. Hurtak

As you know, we do not speak for Ms. Hurtak, whose device(s) and data were also seized by the agents. We will communicate with Ms. Hurtak's counsel about contacting you for the return and/or remediation of the data and drives related to her client.

F Return of The Streaming Video Files/Journalistic Work Product

Based on the allegations of violations of 18 USC 2511 in the warrant, we have presumed that your investigation concerns allegations that Mr. Burke's collection, storage, and publication of video "live feeds" from the Internet violates the federal wiretap and electronic surveillance statute, and that the manner in which he obtained these live feeds violated the CFAA because he, in some way, accessed a computer or computers "without authorization" in order to obtain access to these live feeds and/or that these live feeds were not publicly accessible.

You have indicated that you do not intend, at this time, to return to Mr. Burke (or his counsel) any data or information about these "live feeds," including the live feeds themselves. You likened these live feeds to stolen personal information like Social Security Numbers or medical records obtained and used by fraudsters unlawfully, which you routinely refuse to return to the fraudsters during the scope of the investigation.

Putting aside the question of whether there was probable cause to believe that the live feeds were evidence of any crime (as you know, we wholeheartedly believe that they are not) or whether they were unlawfully obtained (again, we believe the evidence shows that they were not), the live feeds themselves are not "stolen" information, or information obtained by fraud. The live feeds are, in fact, Mr. Burke's journalistic work product. They are the raw materials from which Mr. Burke reports. They are Mr. Burke's "Pentagon Papers" if the Pentagon Papers were not classified, and were obtained lawfully as opposed to having been taken without authorization by Dr. Ellsberg. Many of the seized "live feeds" contain newsworthy content about which Mr. Burke and other journalists have reported, or intend to report on in the future. It is through these "live feeds" that Mr. Burke has developed his reputation as a reporter.

Most significantly, these live feeds are not "stolen" or "obtained by fraud" and most certainly are not "contraband." They are not "fruits of a poisonous tree." By seizing the live feeds, you and

your team have been exposed to information about Mr. Burke and others' journalistic decision making process -- a process which itself is protected by the First Amendment. You will know who Mr. Burke's sources are for identifying, finding, and reporting on information in live feeds. You will know who Mr. Burke and other reporters "target" for investigative reporting. You will know what specific programs or information they have decided to report about. You will also know what they have decided not to report about. Even within the live feeds themselves, your access to them (and retention thereof) will tell you what portions of those live feeds Mr. Burke and other journalists have determined to be "newsworthy" and which portions they determine not to be "newsworthy." This winnowing process is the essence of journalism, and we strongly believe that compelled revelation and continued possession and retention by the government of this information constitutes a continuing affront to the First Amendment rights of Mr. Burke and those with whom he works both as a journalist and as a technical advisor to other journalists. Certainly, your "taint team" has been advised of the journalistic and privileged nature of this information in determining what information to hand off to the investigators. I emphasize here that we have absolutely no indication, technical or otherwise, that this information was anything other than lawfully obtained and accessed. We also distinguish your investigation into the method by which the data was accessed (which, again we believe will reveal that the data was accessed lawfully) and the data itself. We reject your presumption that the data was unlawfully obtained and therefore that you can preemptively restrict Mr. Burke's access to it.

This again is where access to the affidavit in support of the warrant is critical. If the magistrate made a judicial finding (or was asked to) that the data from the "live feeds" was more than simply evidence of some crime, but was itself contraband or the fruits of a crime, then I could sympathize with (but still disagree with) your position regarding return of the journalistic materials. Additionally, there is the "publication" problem. As you know, 18 USC 2511 has two separate criminal offenses. The unlawful "interception" in transmission of certain communications which were not configured to be accessible to the public, and the "disclosure" of those unlawfully intercepted communications.

In *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001) the Court held that "the naked prohibition against disclosures [of unlawfully intercepted communications] is fairly characterized as a regulation of pure speech" and that ""state action to punish the publication of truthful information seldom can satisfy constitutional standards." *Smith v. Daily Mail Publishing Co.,* 443 U. S. 97, 102 (1979)."

The information contained in the "live feeds" is a matter of "public significance" and Mr. Burke had, and continues to have a First Amendment right to report on this content -- which implies the right to "disclose" the content about which he is reporting. See, e.g., *Florida Star v. B. J. F.*, 491

U. S. 524 (1989); *Landmark Communications, Inc. v. Virginia*, 435 U. S. 829 (1978). This right is, of course, contingent upon the fact that Mr. Burke himself did not obtain the data unlawfully, which is the essence of our dispute. At this juncture, our problem is with the presumption you are making that the journalistic records in the live feeds were obtained unlawfully, precluding Mr. Burke from publishing information about them, which works as a prior restraint on Mr. Burke's free speech rights. [2] The feeds were public, obtained lawfully, held lawfully, and are Mr. Burke's work product.

For example, on August 18 2011, the Georgetown University men's basketball team was in Beijing playing a goodwill tour game against the Bayi Rockets, a professional squad affiliated with the Chinese military. A game that had already been physical with aggressive play and hard fouls broke out into a bench-clearing brawl in the fourth quarter after a pile-up under the basket; players from both teams exchanged punches, shoves, and at least one folding chair. The fight spilled into the stands as players and spectators tangled in a chaotic scene; it took coaches and officials several minutes to restore order, and the game was called off.[3]

Mr. Burke, using his skills and knowledge of how to access obscure public web broadcasts, acquired footage of the incident from a Chinese social media stream; while that footage was quickly suppressed by Chinese censors within that country, the truth—thanks to Mr. Burke having captured it—was airing hours later on ESPN's *SportsCenter* and on each U.S. network's evening news. He neither sought, nor expected to obtain the explicit "consent" of the Chinese censors to broadcast the previously public feed. He found, on public sites, copies of the stream and preserved them for broadcast by ESPN.

Effectively, by asserting that the video feeds were obtained unlawfully, and refusing to return them, you are restraining Mr. Burke's publication of the newsworthy content in those files. We do not currently know if the magistrate judge who authorized your seizure and examination of

---

[2] *Cox Broadcasting Corp. v. Cohn,* 420 U.S. 469 (1975)(journalists have a First Amendment right to release information found in public domain records); *Near v. Minnesota*, 283 U.S. 697 (1931);(gag order prior to jury impanelment violated the First Amendment); *New York Times Co. v. United States,* 403 U.S. 713 (1971)(government could not restrict the right to publicly report on the contents of stolen classified information in the Pentagon Papers); *Seattle Times Co. v. Rhinehart*, 467 U.S. 20 (1984)(a specific protective order restricting access to or publication of information obtained in civil litigation is enforceable); *Smith v. Daily Mail Publishing Co.* 443 US 97 (1979) (statute restricting publication of juvenile offender's name violates Free Press); and, of course, *United States v. Progressive, Inc.,* 467 F. Supp. 990 (W.D. Wis. 1979)(First Amendment includes the right to publish, without prior restraint, even a "how to" book on creating a nuclear weapon).

[3] Gene Wang, Georgetown basketball exhibition in China ends in brawl. The Washington Post, August 18, 2011 available at https://www.washingtonpost.com/sports/colleges/fight-ends-georgetown-basketball-exhibition-in-china/2011/08/18/gIQAs1zeNJ_story.html ("Xinhua News Agency, China's official news service, did not have an immediate account of the game, and although other prominent Chinese Web sites such as 163.com and sina.com posted stories, government censors shortly thereafter took them down.")

those files similarly authorized this prior restraint on Mr. Burke's publication rights. Indeed, we do not know if the affidavit submitted to the magistrate judge advised the magistrate that the seizure order would act as such a prior restraint. In short, did the FBI tell the magistrate that you were seeking an order to shut down a newsroom to prevent the publication of truthful information of public concern because they believed that this information was "intercepted" unlawfully? Again, access to the affidavit will reveal this. Due Process supports its release.

Your efforts to prevent Mr. Burke from having access to his lawfully obtained work product goes to the core of his First Amendment protected activities. 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."). Your refusal to return Mr. Burke's lawfully downloaded live feeds -- the very information upon which he has built his journalistic reputation and journailistic consulting business is the ultimate "prior restraint." You have seized his newsroom. The Supreme Court has long recognized prior restraints as 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. Cf., *Cooper v. Dillon,* 403 F. 3d 1208, 1216 (11th Cir. 2005)(distinguishing prior restraints which "freeze" speech and post restraints which punish it). There is a "heavy presumption against [the] constitutional validity" of a prior restraint under federal constitutional law, and the party seeking such relief bears the burden to overcome that heavy presumption. *N.Y. Times Co. v. United States,* 403 U.S. 713, 714 (1971) (per curiam). A prior restraint could pass constitutional muster "only" in the most of "exceptional" of cases. CBS, Inc. v. Davis, 510 U.S. 1315, 1317 (1994) (Blackmun, J., in chambers (quoting Near, 283 U.S. at 716)). Indeed, 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), with the Supreme Court making clear that a prior restraint may be contemplated only in the rarest circumstances, such as where necessary to prevent the dissemination of information about troop movements during wartime, *Near*, 283 U.S. at 716, or to "suppress[] information that would set in motion a nuclear holocaust." *N.Y. Times,* 403 U.S. at 726 (Brennan, J., concurring). Accord, *The News-Journal Corp. v. Foxman,* 939 F. 2d 1499, 1512 (11th Cir., 1991).

It is axiomatic that the First Amendment protects Mr. Burke's right to publish information of public concern that it lawfully obtained—even if a court or the government may have had the power to restrict dissemination in the first instance. See *Oklahoma Publ'g Co. v. Dist. Ct.,* 430 U.S. 308, 311–12 (1977) (reversing a prior restraint prohibiting the press from publishing the name of a juvenile defendant, which the journalist had learned by attending a court proceeding,

even though courts generally may protect the identity of juveniles); *N.Y. Times*, 420 U.S. at 714 (holding that a newspaper cannot be restrained from publishing classified documents obtained by the newspaper's source without authorization); see also *Landmark Commc'ns, Inc. v. Virginia,* 435 U.S. 829, 849 (1978) (Stewart, J., concurring) ("Though government may deny access to information and punish its theft, government *may not prohibit or punish the publication of that information* once it falls into the hands of the press, unless the need for secrecy is manifestly overwhelming.") (emphasis added); *Bartnicki v. Vopper,* 532 U.S. 514, 535 (2001) (determining that publication of material obtained lawfully by a publication but unlawfully obtained by its source does not "remove the First Amendment shield from speech about a matter of public concern.").

In this case, Mr. Burke has a presumptive right to publish the works he has collected. A mere unproven allegation that the originator of the original stream did not expressly authorize Mr. Burke to store the stream does not change his right to publish. Any argument that Mr. Burke is prohibited from publishing the live feeds he obtained lawfully because the media outlets that made them public did so "inadvertently" or "mistakenly" is unavailing. See *Florida Star v. B.J.F.*, 491 U.S. 524, 537 (1989) (reversing judgment against newspaper that published name of rape victim inadvertently disclosed in police report). Refusing to return to Mr. Burke his live feed data impermissibly interferes with the media's exercise of its First Amendment rights. See, e.g., *FMC Corp. v. Capital Cities/ABC*, 915 F.2d 300, 305-07 (7th Cir. 1990) (rejecting demand that ABC News return all copies of documents plaintiff alleged were "stolen" from it; court held that ABC was "free to retain copies of any of [the plaintiffs'] documents in its possession [and to disseminate information in them] in the name of the First Amendment."); see also *Smith v. Daily Mail Pul'g Co.,* 443 U.S. 97, 103 (1979) ("[I]f 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 to further a state interest of the highest order."). In the instant matter is appears the Government has unilaterally declared that the live feeds were obtained unlawfully, that they are somehow "stolen" or "contraband" and therefore that they cannot be provided to Mr. Burke, and cannot be published by Mr. Burke or others. If there is information in the affidavit in support of the warrant to support your "contraband" theory to warrant this prior restraint, we are certainly not aware of such information. While your office might be justified in refusing to, for example, return seized contraband (narcotics, CSAM) after a raid, or refusing to provide copies of stolen identity information (PII, SSAN's etc.) in a fraud case until pretrial discovery under F.R.Crim. P. 16, what was seized here was not contraband and was not stolen. It is a journalists' work product.

Moreover, the live feeds Mr. Burke lawfully collected were all formerly in the public domain -- they were all publicly accessible -- irrespective of whether the news, entertainment, sports or

public enterprises published them "on air." Indeed, because "live" feeds must be captured while they are being broadcast "live," part of Mr. Burke's value to the journalistic community lies in his finding, collecting, storing, winnowing, organizing and making available these "stored" live broadcasts. Seizing and refusing to return that which was previously public, in a manner that serves to prevent Mr. Burke and other reporters from reporting on this content is the ultimate "prior restraint," using armed FBI agents to prevent publication.

As you know, compelled disclosure of journalistic work product undermines public trust in the media because it effectively deputizes journalists as investigative arms of the government. To play its crucial role in society, the press must not only be independent, but also be perceived as independent. See *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 571-72 (1980) ("To work effectively, it is important that society's criminal process satisfy the appearance of justice."); *Gonzales v. National Broadcasting Co., Inc.*, 194 F.3d 29, 35 (2d Cir. 1998)(acknowledging "the symbolic harm of making journalists appear to be an investigative arm of . . . the government" and emphasizing the "paramount public interest in the maintenance of a vigorous, aggressive and independent press capable of participating in robust, unfettered debate over controversial matters"). The fact that the producers of the live feeds were not happy that their feeds were accessed and published for newsworthy purposes does not justify any assertion of criminal activity, and certainly does not justify the I seizure and prior restraints occurring here.

G The Operation of "Burke Communications"

In our discussion Friday you indicated that you did not understand "what Mr. Burke did for a living," how he was paid, and the function of Burke Communications. This is understandable, as digital journalism -- particularly in the way it is practiced in 2023 -- differs substantially from the way we old folk (I have you beat by a year) think of journalism. [4]Undoubtedly, however, when you sought and obtained consent from Main Justice to seek a warrant to seize Mr. Burke's newsroom, and when you sought the warrant from the magistrate to seize the newsroom, you or the agents undoubtedly made representations to both the DOJ and the magistrate about the nature of Mr. Burke's digital journalism. I am certain that your representations are fully consistent with what I describe below, since Mr. Burke's activities are well known on the Internet, and any of his tens of thousands of Twitter followers could have told you what he does (and probably did). Once again, what follows is a lawyer proffer and not a statement of my client.

[4] *Steve Jackson Games, Inc. v. United States Secret Service,* 816 F. Supp. 432 (W.D. Tex. 1993)(Privacy Protection Act applied to new forms of electronic communications and journalism like Bulletin Board Services)

Tim Burke is a journalist whose work has essentially defined how news is covered on social media. Among the things he does is to collect "live feed" videos from around the world -- from news studios, sports broadcasters, entertainment venues, and other live streams and stores and mines these live feeds for newsworthy content. Just by way of example, when something newsworthy happens anywhere in the world, the live streams of local broadcasts may show newsworthy content other than that the television station chooses to broadcast themselves. For more than ten years, Tim Burke has compiled the URLs of public web broadcasts he believes to be of potential newsworthiness. These public web broadcasts include those of broadcast and cable news networks, news feeds published by those networks, local TV news broadcast feeds, and those originating from federal, state, and local governments.

One of Tim's specialties is collecting foreign language (e.g., Russian) broadcasts of U.S. sporting events with Russian language commentary, and making portions thereof available to international audiences. In other cases, Burke finds alternate takes or angles of materials which have been broadcast to provide context for, or to dispute the "official" story of what happened in newsworthy events. For example, his access to an alternate feed of the 2022 Academy Awards enabled him to report what had been censored on ABC in the United States: that actor Will Smith slapped presenter Chris Rock due to Smith taking issue with a joke at his wife's expense.[5] Similarly, his access to an international broadcast of the Bills-Bengals Monday Night Football game this past season enabled Burke to provide reporting that refuted the NFL's official statement about its actions in the wake of Bills safety Damar Hamlin's devastating on-field injury.

To do this, Mr. Burke scours the public Internet [6] for web addresses of PUBLIC broadcasts of live streams. Using various public domain search tools, among other things, he looks for files with the suffix "m3u8" which is an Internet protocol similar to HTTP (HyperText Transfer Protocol) which defines the Moving Picture Experts Group [MPEG] Audio Layer 3 Uniform Resource Locator. Searching for m3u8 files locates streaming video (and audio) files in the same way that searching for .pdf files finds files compatible with Adobe Acrobat Portable Document Format, or searching for .docx finds files compatible with Microsoft's Word/Office suite. Similarly, the "IPTV" format, or "Internet Protocol Television" protocol is also used to stream live video. IPTV is widely deployed in subscriber-based telecommunications networks with high-speed access channels into end-user premises via set-top boxes or other customer-premises equipment. IPTV is also used for media delivery around corporate and private networks. IPTV in the telecommunications arena is notable for its ongoing standardization process (e.g., European Telecommunications Standards Institute). IPTV services may be classified into live television

[5] https://www.youtube.com/watch?v=myjEoDypUD8&ab_channel=GuardianNews
[6] This is to distinguish the "public Internet" from the unindexed "dark Web," although the distinction between the two is more a matter of semantics than a technical distinction.

and live media, with or without related interactivity; time shifting of media, e.g., catch-up TV (replays a TV show that was broadcast hours or days ago), start-over TV (replays the current TV show from its beginning); and, video on demand (VOD) which involves browsing and viewing items of a media catalog.

The process for searching for, locating and storing live video feeds does not differ fundamentally from other forms of Open Source Intelligence (OSINT) commonly used by computer security researchers, web researchers, law enforcement agencies, threat intelligence firms, historians, sociologists, and of course, journalists. It is as much an art as a science -- including knowing how to look, what to look for, and what is likely to be significant and what is likely to be trivial. It also involves a winnowing process, a selection process, and the collection of massive amounts of streaming data. Since you have had access to Mr. Burke's newsroom for more than nine weeks, you can see that there are tens of thousands of such live streams that Mr. Burke has painstakingly compiled, organized and indexed. He is, frankly, the best in the business.

In addition to simple web searches (such as on Google or other similar search engines) Mr. Burke also habitually and persistently checks to see if any video he views in a browser is accessible to the public; scanning public lists of web broadcasts on Github, forums, Telegram channels, and simply through Google; and through communication with fellow journalists and sources. He is well connected in the field of digital journalism, and well respected there as well. Mr. Burke uses free, open-source software including Streamlink, [7] the tool used to record public web broadcasts, and VLC, [8]the tool used to view them. All of these tools are public, open source, and perfectly lawful. They are tools to display or view content -- not hacker tools.

What you have seized represents tens of thousands of man-hours of work by Mr. Burke and his fellow digital journalists, simply in identifying sources alone. It also represents myriad hours in the process of downloading, compressing, editing, formatting, organizing, and determining what is newsworthy. In short, journalism.

H Burke's Work With Other Journalists

Mr. Burke and by extension, Burke Communications, works with other journalists and outlets in several ways. First, Mr. Burke educates, trains and coaches other journalists in how and why to find, use and incorporate live video content into their work. Second, Mr. Burke acts as a resource for these other journalists -- providing them with access to his vast repository of streaming

[7] https://streamlink.github.io/

[8] VLC stands for "VideoLAN Client." It is an open source media player software that is part of VideoLAN, an academic project for streaming video that began in Paris in the mid-1990s. VLC runs under all popular operating systems and supports a wide variety of video formats. https://www.videolan.org/vlc/download-windows.html

content, live streams, URL's or addresses of streams, as well as edited or organized content. Thus, for example, if a fellow journalist were looking for time-stamped footage of the exterior Oval Office door to confirm reporting of the President being within, Mr. Burke could scan his archives for the tell-tale presence of a U.S. Marine guarding that door at the specified time, or help the journalist locate such footage. Third, when Mr. Burke finds streams of newsworthy content, he works with journalists and other news outlets to broadcast/publish the newsworthy content. As you already know, the information about the Carlson/Kanye interview was broadcast by news organizations with which Mr. Burke has a formal or informal relationship. Additionally, other journalists serve as sources of information to Mr. Burke, providing him with newsgathering ideas, story ideas, as well as potential sources for information. Finally, Mr. Burke has developed his own proprietary sources for information, confidential news sources, and even confidential relationships with members of the public on secure social media (DM's) about story ideas and places to search.

As his work with Burke Communications includes teaching other journalists how to identify and monitor those feeds in order to identify when breaking news is imminent or occurring, and then how to record and process those feeds into reporting breaking news. Herecognizes the value and importance of compiling and organizing web broadcasts that are accessible to the public and thus, also, his clients. His efficiency and effectiveness is not a crime.

This approach is important from a journalism perspective as he records the content in its native, raw format thereby ensuring the strictest veracity in his ability to report news as it actually happened.

As there are far more web broadcasts in existence than could reasonably be monitored live, Tim is able to selectively record and archive web broadcasts for long-term storage. This resource has been utilized by his fellow journalists numerous times, with examples ranging from simple time-stamping of when a news event occurred to confirming activities in the Oval Office. On occasion, news organizations that originated the footage themselves have inquired as to whether he had it archived, as they themselves no longer had the raw content. He has worked with organizations like CNN, ESPN, and the NFL to help augment their own content with better quality versions.

His archive of content related to the 2020 COVID-19 outbreak, George Floyd protests, and presidential election as well as his extensive coverage of the events surrounding January 6th is likely only rivaled by CNN (and then, often because CNN regularly airs video taken from his Twitter posts). Journalists and media organizations regularly inquire if "he has saved somewhere" footage of a newsworthy event in the past.

His viral Sinclair Broadcast Group "Extremely dangerous to our democracy" video, [9]seen more than 100 million times, earned him a National Magazine Award nod, and he now both maintains his own digital newsroom—one he utilized to cover events around the country during the 2020 George Floyd protests, and in Washington on January 6th—and works with other journalists and newsrooms to share his expertise and workflows in order to facilitate faster and more accurate news coverage around the world.

After leaving the position of Director of Video at the Daily Beast, he founded Burke Communications, a company that works with news organizations to enhance and augment their reporting capabilities, while regularly doing reporting work himself while under contract to those organizations.

His contracts with those news organizations—which include Heartland Signal, Recount Media, The Dogwood, Up North News, The 'Gander, Cardinal & Pine, and The Keystone—regularly run for months or years during which he becomes part of the newsroom, training new staff on news gathering techniques and, in particular, his proprietary workflow of combining open-source software tools and public web broadcasts to enable journalists to quickly report multimedia breaking news as it is happening. From the U.S. Capitol, to state legislatures, to municipal government, many of the most memorable and important clips of viral news coverage on social media have been produced by journalists trained by Burke Communications—or by Tim Burke himself, whose Twitter account features more than 100,000 followers (some of whom are this country's best known television journalists). His work as a journalist has been featured on every major cable news network, ESPN, *The Daily Show*, and *Last Week Tonight with John Oliver*. Burke Communications regularly provides assistance to cable news networks free-of-charge when they are seeking a particularly elusive news clip or need a higher quality copy of one.

Burke Communications has worked with these networks, as well as rights holders like professional sports leagues and Learfield/IMG, to provide higher quality video of significant events than they themselves are capable of providing. The reasons those organizations request his assistance range from news coverage to social media promotion to video analysis.

What all of these activities have in common is the fact that the live streams collected, stored, analyzed and disseminated -- ALL OF THEM -- are publicly streamed. Indeed, they have to be. When a browser is pointed to a m3u8 file that is NOT public, it is encrypted and cannot be viewed. These encrypted streams would be useless to Mr. Burke. There was no "cracking" or

[9] Erin Nyren, Sinclair Broadcast Group Faces Backlash Over Scripted Promos: 'This Is Extremely Dangerous to Our Democracy' Variety, Apr 1, 2018 available at https://variety.com/2018/tv/news/sinclair-promos-backlash-1202741019/

"hacking" of any of these encrypted feeds as far as we can tell. The live feeds were publicly accessible, internet addressable, and available to ANYONE who could find their location and the appropriate URL.

I Pace of Forensics

You indicated that this case is "not your priority" and "not your most important case." I do not have any reason to question this assertion. It is, of course, Mr. Burke's most important case. We are deeply concerned about the pace of your forensic investigation. In more than ten weeks, the FBI apparently had been unable to make an image of an iPhone because, as you noted, the phone is "locked" and the tools the FBI uses are, as you described, "a generation behind" the latest Apple Operating System (iOS) version. Again, we decline to decrypt the phone to assist you in accessing Mr. Burke's journalistic files.

More frustrating (probably to both of us) is the fact that the hard drives and the contents of the other computers seized apparently have not yet been forensically imaged. While we appreciate your offer to have a "rolling production" of imaging drives, the seized materials should have been -- and indeed could have been -- forensically imaged within days or a week. Apart from resources issues, what appears to be holding this back is your insistence that the imaging for return exclude the publicly accessible video feeds or indeed any information on the drives that is potentially relevant to the investigation. It's not simply that we need this information for the defense -- we fully understand the ordinary timing of discovery in criminal investigations. It is the fact that, because no crime occurred (and the public nature of the seized live feeds will demonstrate this fact), it is our emphatic position that, not only should no warrant have been issued, none should have been sought, and none should have been approved by the Department of Justice under its media guidelines. In short, Mr. Burke should not have been a "suspect"of a crime, and the "suspect" exception to the media guidelines should never have been applied. We understand that you are of a different view, but we cannot have a meaningful discussion on this fact without either (a) access to the affidavit; (b) access to the relevant seized materials; or some disclosure about the evidence leading you to the conclusion that accessing public information is "hacking" and "wiretapping".

II. Substantive Considerations

These concerns are all procedural. More significant are our relentless efforts to resolve the substance of the matter quickly. As I have repeatedly emphasized to you, despite the magistrate's finding of probable cause to conduct the search of Mr. Burke's office/residence and the seizure of his newsroom, Mr. Burke committed no crime and engaged in no behavior which violated either

the CFAA or the wiretap statutes. This is even more significant because, under the Privacy Protection Act, there is a threshold requirement of specific types of criminal behavior by the journalist as a prerequisite for even seeking a warrant to seize a newsroom. In this case, based on the facts as we know them, this threshold has not been, and cannot be met. Again, you have declined to tell us *why* you think Mr. Burke violated the CFAA or the wiretap law, and have adamantly insisted that disclosure to Mr. Burke of the affidavit in support of the warrant would cause some unspecified harm to your investigation. Each time I present our position that no crime occurred, you note that you "understand" our position, but that you nevertheless intend to further investigate.

A. There Was No Violation of CFAA

We have similarly continued to investigate. Our further investigation of both the facts and the law as we know them indicate that this is not a close case. Mr. Burke accessed publicly accessible live streams by simply finding and putting in the appropriate URL for the website. There was no "hacking," no "forced entry" and no special tools necessary.

You have indicated that you are continuing to investigate by speaking to "victims" other than Fox News. We emphatically insist that there are no "victims" because there was no crime. Even if the entities streaming the video were unaware that the videos were publicly accessible, and indeed even if they had no intention of making the videos publicly accessible ("facts" which we emphatically dispute), there was no intentional access to ANY computer "without authorization," and no intentional access to ANY computer in "excess of authorization."

The only cases we are aware of where a prosecutor has taken the position that access by a journalist to publicly accessible information for the purpose of publishing this information was charged as a crime did not end well for the government.

For example, when First Amendment advocates in the City of Fullerton found out that the city's cloud-based "drop-box" had been configured to permit anyone to download municipal files and proceeded to publish these documents, the city alleged that the advocates had "hacked" the city website, and obtained warrants to seize the evidence of the hacking. [10] There, as here, the government asserted that the advocates "should have known" that the records were not intended to be public. Ultimately, the city paid the legal fees and damages of the advocates, and returned most of the seized documents.

[10] *City of Fullerton v. Friends for Fullerton's Future, , et al*., Orange County Superior Court Case No. 30-20\9-01107063-CU-NP-CJC.

Similarly, when a political opponent of then-California Governor Arnold Schwarzenneger accessed the governor's website through a process called "backwards browsing" [11] and found hidden audio files of the Governor and published them, he was similarly threatened with prosecution under the same theory the government may have posited here -- that the publisher "should have known" that the files were not intended to be public. [12] Similar threats to prosecute journalists have been rejected, for example with respect to online journalist [13] Jonathan Albright, who exploited a vulnerability in the CrowdTangle tool that allowed him to access thousands of Facebook sites through an API which was "an unintended way to access information about deleted content" and scrape data about Russian interference with the 2016 Presidential election.

Finally, there is the case of San Francisco journalist Bryan Carmody, whose newsroom and materials were seized pursuant to a search warrant based on allegations that he improperly obtained a confidential police report about a high profile murder. The SFPD and FBI, in violation of DOJ policy, seized Carmody's electronic office, shut down his publication, and, when he obtained access to the affidavit in support of the search warrant which the government sought to keep sealed, Carmody learned that the magistrate was never told that Carmody was a journalist and that the search involved protected activity. [14]

Each of these cases involved a journalist doing their job. Searching for and finding newsworthy content and publishing. In each of these cases, law enforcement agents sought to punish the journalists by asserting that they violated computer hacking statutes because they "should have known" that the publicly accessible data was not intended to be seen, and therefore that they "accessed" the computers containing that data "without authorization." As with Mr. Burke, these searches were unlawful, and the theory of criminality unsupported.

---

[11] Despite the fact that the login page to the site displayed a warning page warning that "unauthorized access is strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 or other applicable laws…" (Id., p. 5, Par. 25, p 31 with contents of banner), and that use of the system was reserved "to authorized users for authorized use only.." (Id.), a user who accessed the website through "backward browsing" (or scraping content that the user did not know was publicly accessible) was not liable for a violation of the California equivalent of the CFAA. The report (Id., p 5) concluded that backward browsing "is a process that is a common practice in the media" for finding information not intended for publication, and included the conclusion of the Deputy Attorney General of California that such access, while not formally authorized, "would not be considered a crime." (Id., p. 5).

[12] Memorandum from CHiP to S. Kennedy, Chief of Staff, Office of the Governor, Governor's Office Computer System Investigation, February 1, 2007, available at https://www.fullertonsfuture.org/wp-content/uploads/2020/09/Governors-Office-Computer-System-Investigation-020107.pdf

[13] ISSIE LAPOWSKY, Shadow Politics: Meet the Digital Sleuth Exposing Fake News, Wired Magazine, BACKCHANNEL JUL 18, 2018 available at https://www.wired.com/story/shadow-politics-meet-the-digital-sleuth-exposing-fake-news/

[14] In the Matter of Brian Carmody, Dkt. No. 2516765 (Cal. Sup. Ct., County of San Francisco, August 2, 2019). Available at https://firstamendmentcoalition.org/wp-content/uploads/2019/08/JudgeHiteOrderQUASH_UNSEAL.pdf

B. Interpretation of the CFAA To Prohibit Access to "Non-Obvious" URLs of Live Video Streams Is Unsupported by the Language of Purpose of the Statute and Constitutes an Affront to the First Amendment

Again, without access to the affidavit in support of the warrant, we do not know why you think Mrl Burke's clicking on public links and visiting public websites is a crime. You have repeatedly declined to advise us of ANY activity undertaken by Mr. Burke or others that is anything other than accessing publicly accessible live streams, and we are aware of no such conduct by him or by others.

Interpreting the CFAA to impose liability for routine newsgathering clearly raises constitutional concerns. Without access to the affidavit in support of the warrant, we can only guess about your theory of why Mr. Burke's access to and dissemination of publicly accessible live feeds constitute a crime. However, we posit that your theory is that accessing these live feeds is illegal—even though any computer user could type that URL into their browser and access the m3u8 files without a password—because the entities streaming the live feeds did not know the data was accessible and because the URLs themselves were not advertised as being accessible by the streamers themselves.

In essence, that entities like Fox News and other entities publicly streaming video were entitled to rely on the fact that the websites streaming the service were not well known, and somehow that Mr. Burke "should have known" that he was "not expressly authorized" to access and report on the contents of the streaming services. Nothing in the "without authorization" provisions of the CFAA requires an individual to demonstrate an invitation to visit an address accessible "to anyone with an Internet connection." *hiQ Labs v. LinkedIn Corp*. 938 F.3d 985, 1002 (9th Cir. 2019)("hiQ Labs I"). *Van Buren* makes clear that improper purpose alone is insufficient for a remedy under the CFAA and instead requires that the information obtained via computer constitute information for which the user has not been granted access. See *Van Buren*, 141 S. Ct. at 1653.

Website operators routinely expose newsworthy information about themselves 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 in the public interest. Take, for instance, web-scraping: the automated process of pulling large amounts of information from websites. Scraping typically does not expose any information beyond what could be found through the manual use of the website; its chief advantage is that it "speeds up the tedious job of manually copying and pasting data into a

spreadsheet, making large-scale data collection possible." [15] But the results, taken together, may reveal more than any one user visiting the website would have noticed. Reporting of this kind has been used to expose grave public failings and unlawful private discrimination.[16]

Understandably, the subjects of stories like these would like the power to suppress them. As a result, websites now routinely purport to forbid scraping, or otherwise using the information they host for research purposes, in their terms of service even as the information itself remains on public display.[17] Sites may wish to attempt to tell journalists like Mr. Burke which information they may or may not gatheron the open internet. As the Ninth Circuit recently noted on remand from the Supreme Court in *hiQ Labs, Inc. v. LinkedIn Corp*. 31 F. 4th 1180, 1196 (9th Cir., 2022)(*hiQ Labs* II) ,"Where the default is free access without authorization, in ordinary parlance one would characterize selective denial of access as a ban, not as a lack of "authorization." Mr. Burke was neither banned from accessing these live streams, nor did he access them without authorization.

The view that entities like Fox News didn't want Mr. Burke to see the publicly accessible live feeds and that Mr. Burke "should have known" this is unworkable. Private preferences cannot determine liability for routine, First Amendment newsgathering. If that were the case, subjects of journalistic investigations could simply decide to make such reporting unlawful. Consider the civil-rights testing and accountability journalism that inspired the 1988 amendments to the Fair Housing Act.[18] If conducted today, much of the data collection would take place through scraping and other online data journalism techniques. The subjects of such reporting could simply make such reporting illegal by invoking the CFAA. Not only would that result chill reporting in the public interest, but also it would raise serious questions as to whether each law is void for vagueness— "unworkable and standardless"—because they make "each webmaster into its own legislature." *Sandvig v. Barr* 451 F.Supp.3d 73, 88 (D.D.C. 2020)("*Sandvig*").[19] In fact, the case here is more egregious than that of either *Sandvig*, *hiQ*, or *Nosal*, because in Mr. Burke's case, unlike these cases, there were no "Terms of Service" or "Terms of Use" violated or circumvented by Mr. Burke in his reporting. Entering the appropriate URL brought up the streaming content without any contractual limitation or circumvention.

---

[15] Note, Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision (2020) 120 Colum. L.Rev. 131, 137.

[16] See, e.g., Zarkhin & Terry, Kept in the Dark: Oregon Hides Thousands of Cases of Shoddy Senior Care, Oregonian/Oregonian Live (Apr. 22, 2019)<https://perma.cc/BKL4-6GRD>; Yachot, Your Favorite Website Might Be Discriminating Against You (June 29, 2016) ACLU <https://perma.cc/6W67-68J4>.)

[17] See Note, supra, 120 Colum. L.Rev. at p. 134.

[18] See Rottman, Knight Institute's Facebook 'Safe Harbor' Proposal Showcases Need for Comprehensive CFAA Reform (Aug. 6, 2018) Reporters Com. for Freedom of the Press <https://perma.cc/34C3-DJRE> [as of July 17, 2023] [citing Dedman, The Color of Money, Atlanta Journal-Constitution (May 1–4, 1988)]

[19] Orin S. Kerr, Vagueness Challenges to the Computer Fraud and Abuse Act, 94 Minn. L. Rev. 156, 1576 (2010)

Your proposed extension of the CFAA to criminalize access to that which is accessible to the public because the subject of reporting is embarrassed by what is found is precisely the kind of unjustified extension of the law rejected by the Supreme Court in *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." [20]As the Supreme Court noted this term in *Dubin v. United States,*[21] "[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." [22] As the *Van Buren* court noted in rejecting a similarly expansive view of the "exceeds authorized access" language of the CFAA, "[t]he Government's approach would inject arbitrariness into the assessment of criminal liability." *Id*. at 1662. This is even more true where, as here, the broad interpretation offered by the government would implicate First Amendment rights of speech and of the press not only of Mr. Burke but of all journalists. [23]

There is no authority for the proposition that a resource deliberately published to the open internet remains "private" if the owner chooses not to advertise that information is hosted there. This theory, too, threatens to chill routine journalism. It would turn ordinary Internet searches into crimes. In one case, for example, a reporter's clever Googling revealed that a phone company had exposed reams of its customers' personal data "on unprotected Internet servers that anyone in the world could access," leading the Federal Communications Commission to launch its own investigation.[24] Reporters routinely find newsworthy information by simply looking for it on public -- if not well broadcast -- websites and locations.

---

[20] In *Van Buren,* the government argued unsuccessfully to the Court that the fact that the CFAA required the government to prove that the unauthorized access was "intentional" limited prosecutions to egregious cases. As Mr. Burke's case demonstrated, it does not. As the Supreme Court noted in *Van Buren*, "the Government's current CFAA charging policy shows why Van Buren's concerns [of misuse of the statute] are far from "hypothetical," Id, at 1661-62.

[21] Dkt. No. 22–10, June 8, 2023, *Slip Op*., 17-18 (citation omitted)

[22] Id. citing *Van Buren*

[23] Courts have consistently 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 *Sandvig v. Barr*, 451 F. Supp. 3d 73, 88–89 (D.D.C. 2020) ("Plaintiffs' First Amendment challenge raises such risks . . . and thus weighs in favor of a narrow interpretation under the avoidance canon."); *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).

[24] See Bowman, FCC Announces $10 Million Fine for Security Breach Following Scripps Investigation (Oct. 24, 2014) ABC Action News <https://bit.ly/2JMazaY> "A federal investigation launched when a reporter's Google search revealed a phone company storing the confidential information of hundreds of thousands of customers on an open Internet site has resulted in a $10 million fine against two carriers.)[as of July 17, 2023].)

Your interpretation of the CFAA -- if, indeed this is your interpretation -- would outlaw that kind of reporting. You would likewise make it illegal for journalists and researchers to investigate even whether the use of nonobvious URLs is an adequate approach to maintaining the privacy of a webpage. This is precisely what security researchers routinely do, and reporters like Brian Krebs at Krebs on Security routinely report on security vulnerabilities found by security researchers searching for precisely these kinds of "nonobvious" URLs, or finding data that is publicly accessible.

Fox News was embarrassed by the broadcast of its own hypocrisy. It was embarrassed by the fact that it held racist, anti semitic and sexist remarks from public view. It was embarrassing because Mr. Burke was able to find and expose information about the Carlson/West interview. It was embarrassed because it had made those feeds available to the public in a way that Mr. Burke could -- and did -- find them and disseminate them. The Academy Awards was embarrassed that it concealed critical information about "the slap." The GOP was embarrassed because, when C-Span "cut away" from the verbal scuffle between Utah Senator Mitt Romney and New York Congressman George Santos [25] -- an exchange not broadcast by C-Span, but found and reported on by Mr. Burke. Chinese censors were embarrassed by the fact that they were caught mis-describing what happened at the game. The fact that these entities would "rather not" have Mr. Burke or other journalists report on what they stream to the public does not make accessing those streams into crimes. In fact, such an interpretation "presents a significant risk" that a constitutional right "will be infringed." *NLRB v. Catholic Bishop of Chicago*, 440 U.S. 490, 502 (1979).

To address just such First Amendment concerns, other courts have concluded that the CFAA should be read to prohibit only the circumvention of certain code-based restrictions—not the violation of site owners' private expectations. See, e.g., *Sandvig*, supra, 451 F.Supp.3d at pp. 88–89. As between "plausible statutory constructions," if one "would raise . . . constitutional problems, the other should prevail." *Clark v. Martinez* 543 U.S. 371, 380–81 (2005). The Department of Justice should have construed the CFAA narrowly to avoid this risk to lawful news gathering in the public interest. The CFAA does not prohibit accessing information that a website owner has chosen to make available to any internet user. To be clear, the CFAA does not, in fact, criminalize routine newsgathering. Instead, when Congress prohibited "access[ing] a computer without authorization," (18 U.S.C. § 1030(a)), it intended to prohibit conduct

[25] Caitlin Yilek, George Santos and Mitt Romney have tense exchange before State of the Union, CBS News, February 8, 2023 available at https://www.cbsnews.com/news/george-santos-mitt-romney-state-of-the-union-2023/ (visited July 15, 2023)

"analogous to . . . 'breaking and entering,'"[26] That is, it prohibited "hacking."[27] Hacking is not what happened here. Journalism is.

Your theory of criminal liability appears to be focused on a misplaced notion that Mr. Burke "should have known" that he was not authorized to access the streaming videos he accessed, and that in some way, the entities about whom he reported using these live videos were "victims" of his "unauthorized access" to the online streams. This is fundamentally based on a misunderstanding of ordinary norms of internet use. [28] 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 -- accessible simply by either clicking a link or putting a URL into a browser window. This is not a crime.

More fundamentally, though, actual notice that a website owner does not appreciate a user's access is not enough to trigger liability under the CFAA, and your proffered theories to the contrary highlight the pitfalls of adopting such an approach. (See *hiQ Labs* I, supra, 938 F.3d at pp. 1001–02.) It is wholly unreasonable to expect a journalist, who finds publicly accessible information on a publicly accessible website or streaming content, to assume that the person or persons who put the content out there "did not know" or "did not want" that content to be publicly accessible simply because the URL is "non-obvious." [29] 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 a 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. As a result, visitors to a specific URL have no way of knowing in the abstract if it was "private" and access to it "unauthorized."

---

[26] H.R.Rep. No. 98-894, 2d Sess., p. 20 (1984); *US v. Nosa*l, 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 (ED 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); .*US v. Aleynikov*, 737 F. Supp. 2d 173, 192 - (SDNY, 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.

[27] *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 "antihacking purpose"O)

[28] 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).

[29] 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"

Equally unavailing is any argument that Mr. Burke's access to the LiveU website was "unauthorized" because Mr. Burke used a voluntarily published credential, found on the open Internet and supplied by the holder of the credential to access the site. Indeed, the credential was a "demo" credential, provided by the website operator to its holder specifically to permit free use of the account, and the account holder chose to share the credential online.

As of this writing, LiveU offers anyone who signs up their own "demo" credentials. We note that Mr. Burke's use of the demo credentials CBS published did not grant Mr. Burke access to any of the Fox News or other streaming content. The use of the demo credentials merely granted Mr. Burke access to the same information ANY user of ANY demo credentials on the LiveU site would have had. When he accessed the LiveU website, the site itself downloaded TO ANY USER the .txt file containing the list of visible and accessible live video feeds. No userid or password was necessary to access these feeds. The list of feeds was available to anyone who logged into the site -- including anyone with any demo account. Access to the live feeds themselves required no userid or password - they were Internet addressable. Again, we are baffled by what your interpretation of the statute could be that would lead to any conclusion that this conduct constituted prohibited "unauthorized access" to or "exceeding authorized access" to a computer, or indeed, whose computer was "accessed" without authorization? The only thing we can think of is that you believe that it is unlawful for users to use voluntarily shared credentials where, as here, there is nothing in the LiveU terms of service that prohibit it. Alternatively, you may be asserting that Mr. Burke "should have known" that the CBS station's publication of its demo credentials was inadvertent or accidental -- something that is absurd for Mr. Burke to have assumed, particularly since the sharing of "demo" credentials is commonplace.

C. There Was No Violation of the Wiretap Statute

We similarly fail to see why viewing or downloading publicly accessible video live streams implicates much less violates the wiretap statute, 18 USC 2511. The Eleventh Circuit addressed precisely the question of whether one violates the wiretap statute when one accesses communications that are configured to be accessible to the public. In S*now v. DirecTV, Inc.,* 450 F. 3d 1314, 1320-21 (11th Cir., 2006), the Court noted that the purpose of the amendments to the wiretap law to include "electronic communications" was "to protect the privacy of the growing number of electronic communications. See 132 Cong. Rec. H4039 (1986) (statement of Rep. Kastenmeier)." Mr. Burke's viewing of publicly accessible live streams did not implicate such privacy concerns. Indeed, it is unreasonable to think that any of the participants in the broadcasts -- sitting in front of banks of cameras, knowing that their communications were being both recorded and broadcast -- had what any court would conclude to be a "reasonable expectation of

privacy" in the contents of what they were broadcasting. Moreover, however, there was no "interception" of these communications. They were being broadcast and streamed. He no more "acquired the contents" of communications by clicking the live stream links than one "acquires the contents" of a television broadcast by turning on the TV.

The *DirectTV* court went on to note that:

> Since its inception, the ECPA provided "several clear exceptions to the bar on interception so as to leave unaffected electronic communication made through an electronic communication system designed so that such communication is readily available to the public." 131 Cong. Rec. S11790-03 (1985) (statement of Sen. Leahy on a bill that was the precursor to the ECPA); see also 131 Cong. Rec. E4128 (1985) (statement of Rep. Kastenmeier on the same bill).
>
> Indeed, the ECPA explicitly reads, "It shall not be unlawful under this chapter or chapter 121 of this title for any person—(i) to intercept or access an electronic communication made through 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) (emphasis added). Chapter 121 refers to the SCA. ECPA § 201. The legislative history and the statutory structure clearly show that Congress did not intend to criminalize or create civil liability for acts of individuals who "intercept" or "access" communications 1 that are otherwise readily accessible by the general public.

Id.

This is what Mr. Burke did. As the Eleventh circuit explained, "If by simply clicking a hypertext link, after ignoring an express warning, on an otherwise publicly accessible webpage, one is liable under the SCA, then the floodgates of litigation would open and the merely curious would be prosecuted. We find no intent by Congress to so permit. Thus, the requirement that the electronic communication not be readily accessible by the general public is material and essential to recovery under the SCA." *Id*.

Mr. Burke accessed unencrypted, publicly accessible, Internet addressable live video feeds by "simply clicking on a hypertext link…" No userid or password was required. The feeds were configured to be accessible to the public, and Mr. Burke accessed them in furtherance of his First Amendment protected activities. This plain and simple is not a crime.

D. Possible Failure to Follow PPA and DOJ Guidelines in Conducting Searches of the Media

Perhaps most troubling is our perception that your office has "conjured" a criminal offense where there was none in order to declare Mr. Burke as not being protected under the myriad laws and policies prohibiting searches with respect to journalists, but rather to label him a "subject" of the investigation and thereby permitting the issuance of a search warrant which would otherwise be prohibited by law. We find this deeply troubling, and invariably chilling on the rights of the press. Without access to the affidavit in support of the warrant, we have deep concerns about whether the required personal approval of the Attorney General to obtain a warrant for the premises of a news media entity was sought or obtained, whether the DAAG of the Criminal Divisions and/or the Attorney General considered the "close question" of whether Mr. Burke's activities were "newsgathering" activities under the regulations, and whether the affidavit specified the precise manner in which the searches were to be minimized and the use of a Special Master or taint team to protect the materials that were covered by Mr. Burke's journalist privilege under Florida and Federal law.

There are at least ten major restrictions on the ability of the government to seek, and the courts to issue search warrants which implicate First Amendment-protected newsgathering operations. These include (1) the federal Privacy Protection Act [30]; (2) DOJ Regulations [31] (3) The Department of Justice Manual[32]; (4) the "Garland" Memo;[33] (5) the Computer Crime and Intellectual Property Section Guide on Seizure of Electronic Records ("the CCIPS Guide")[34]; (6) the U.S. Constitution;[35] (7) the Florida Constitution; [36] (8) Florida statutory privilege [37]; (9)

[30] 42 U.S.C. 2000aa(a)(1) et seq.
[31] 28 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
[32] United States Attorneys Manual 9-13.400
[33] 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
[34] 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
[35] U.S. Const., Amend I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press;")
[36] Fl. Const. Art II Section 4 "Freedom of speech and press.—Every person may speak, write and publish sentiments on all subjects but shall be responsible for the abuse of that right. No law shall be passed to restrain or abridge the liberty of speech or of the press."
[37] Fl. Stat. 90.5015

federal common law of privilege[38] ; and (10) applicable case law. In short, the search of Mr. Burke's office, and the seizure of his newsroom is an anathema to every principle behind the First Amendment and should only have been requested – and only have been approved – after having exhausted every other reasonable remedy, and upon the highest showing of need. As the Garland Memo itself notes:

> A free and independent press is vital to the functioning of our democracy. 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 from certain law enforcement tools and actions, whether criminal or civil, that might unreasonably impair newsgathering. The policy is not intended to shield from accountability members of the news media who are subjects or targets of a criminal investigation for conduct outside the scope of newsgathering.[39]

We understand from your cryptic comments about having to have companies of your work "reviewed" by Main Justice, and your representation that you have to file a lot of paperwork with Main Justice in this case, that this is because of the need to comply with the provisions of the Privacy Protection Act, and the DOJ Guidelines on searching and seizing computers related to members of the media.

We can both agree that seizing a journalist's email records by targeting him as a suspect in a national security investigation was possible because of a loophole that exists under the "suspect exception" of the Privacy Protection Act ("PPA"), which generally protects journalists from having to hand over work product in criminal investigations. Under the PPA, the Justice Department can obtain a warrant against a reporter to, as here, seize "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…" if and only if

---

[38] See, e.g., F.R.E. 501, Riley v. City of Chester, 612 F.2d 708, 713-16 (3d Cir. 1979)(recognizing a federal common law journalist privilege); In re Williams, 766 F. Supp. 358, 367-69 (W.D. Pa. 1991) aff'd by an equally divided en banc court, 963 F.2d 567 (3d Cir. 1991); Gulliver's Periodicals, Ltd. v. Chas. Levy Circulating Co., 455 F. Supp. 1197, 1201 (N.D. Ill. 1978) ("[C]ourts have fashioned a testimonial privilege which inures to the benefit[] of news gatherers and enhances the free flow of information to the public at large."). United States v. Cuthbertson, 630 F.2d 139 (3d Cir. 1980); Accord, The Federal Common Law of Journalists' Privilege, Association of the Bar of the City of New York, Committee on Communications and Media Law, available at https://www.nycbar.org/pdf/report/White%20paper%20on%20reporters%20privilege.pdf

[39] DOJ guidelines make it clear that "newsgathering" includes the receipt of information -- including stolen information or classified information -- or establishing the means of receiving such information, "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."

"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" [40]42 U.S. Code § 2000aa. There is no doubt that Mr. Burke has such a purpose, and that what was seized and sought to be seized were his work product materials. We challenge, based on our understanding of both the facts and the law in this case ANY assertion of "probable cause" to believe that an offense "to which the materials relate" was committed when Mr. Burke accessed publicly available information. In short, the warrant not only should not have been issued, it should not have been sought.

If, however, we look at how the DOJ has traditionally handled applications for search warrants or subpoenas to journalists they have only been used to investigate criminal activity by journalists outside the scope of newsgathering activities. Each year, DOJ issues a report on the number of times it has sought information from or about journalists (including subpoenas, warrants or demands to third parties like ISP's, email providers, etc.). These reports contain summaries of how DOJ obtained approval for, and utilized compulsory process for information about reporters. Each year, there are only a handful of such cases reported. The 2019 report [41] indicated one instance in which the government investigated a reporter in connection with newsgathering activities, but later determined that "the target was not in fact a member of the news media at the time of the criminal conduct under Investigation." *Id*., at p. 1. The other cases noted in the report involved searches of journalists suspected of participating in an extortion scheme that "was not based on, or within the scope of, newsgathering activities," three instances of the issuance of a search warrants or other process for electronic media of a "member of the news media suspected of receipt, distribution, and possession of child pornography" outside the scope of newsgathering, and two instances of obtaining warrants for an investigation of a journalist for stalking and cyberstalking "not based on, or within the scope of, such individual's newsgathering activities." *Id.,* p. 3.

There is not a single case like that of Mr. Burke where the government sought to peg the journalist as a criminal for obtaining newsworthy content. This case appears to be *sui generis*.

---

[40] We note parenthetically that, if you are relying on the "disclosure" provisions of 18 U.S.C. 2511 as the criminal behavior that justifies a search under the PPA, the statute provides that "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 withholding of such materials or the information contained therein.." Id. Thus, if the crime is the communications to others by Burke of the materials, the search is prohibited under the PPA, and those who sought the warrant could have civil liability thereunder.

[41] Department of Justice Use of Certain Law Enforcement Tools to Obtain Information from, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media, Annual Report: Calendar Year 2019, available at https://www.justice.gov/file/1429846/download

The 2020 report [42] speaks about the Trump administration issuing subpoenas for records of reporters (including those at the New York Times) for cell phone and email records in an effort to track down a federal leaker, who'd reportedly offered the reporters details about contacts between the Russian ambassador and high-ranking members of the Trump campaign, and numerous examples of the government seeking information from journalists about courthouse arson investigations -- presumably arising from the Black Lives Matter protests. The 2020 report also includes several compulsory process demands in connection with national security leak/espionage cases. The only noted demands to reporters in 2020 was a subpoena for documents related to an investigation of "harassment directed towards a member of the news media" a "subpoena to a radio broadcast entity for records related to alleged false claims made by a radio personality regarding products being sold on the personality's website" and "a tax fraud investigation, … not related to newsgathering activities. The 2021 report [43] indicates a change in how the new administration sees compulsory process to journalists, including seeking information in the hands of journalists about the January 6, 2021 attack on the U.S. Capitol. The 2021 report describes voluntary compliance by members of the media with investigators of the insurgency; the feds did obtain grand jury subpoenas for journalists — but only, it says, after these reporters "agreed in advance to comply."[44] Here, however we see the first cases in the report of DOJ seeking to use the "suspect" exception to the PPA and the DOJ policy, but again, these cases related to allegations that a reporter conspired with a government official and a former member of congress to engage in insider trading activities, that a reporter was involved in money laundering activities, that a reporter was involved in child exploitation, [45]and that a reporter was involved in stalking. All of these activities are clearly outside the scope of what Mr. Burke is alleged to have done -- obtained newsworthy information with the intent to publish it.

In short, I can find no cases in which a journalist like Mr. Burke was targeted for investigation by the Department of Justice because of the method by which he or she collected information for reporting to the public. It appears to be unprecedented. [46] When there is a "close or novel"

---

[42]Department of Justice Use of Certain Law Enforcement Tools to Obtain Information from, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media
Annual Report: Calendar Year 2020 available at https://www.justice.gov/criminal/page/file/1429906/download

[43] Department of Justice Use of Certain Law Enforcement Tools to Obtain Information from, or Records of, Members of the News Media; and Questioning, Arresting, or Charging Members of the News Media, Annual Report: Calendar Year 2021available at https://www.justice.gov/criminal-fraud/file/1534096/download

[44] Id., p. 3.

[45] This oblique reference is apparently a reference to an investigation of ABC News Reporter Gordon Meek who was charged in the Eastern District of Virginia with transportation of child pornography. https://www.justice.gov/opa/press-release/file/1566416/download David Folkenflik,The FBI raided a notable journalist's home. Rolling Stone didn't tell readers why, NPR News, March 21, 2023, available at https://www.npr.org/2023/03/21/1164360143/rolling-stone-fbi-raid-journalist-james-gordon-meek

[46] A reporter for the St. Louis Post Dispatch was threatened with State criminal prosecution for revealing the fact that certain Missouri government websites were vulnerable to hacking. Rachel Treisman, A Missouri newspaper told the state about a security risk. Now it faces prosecution, NPR News,

question about whether a member of the news media is acting within the scope of newsgathering, that determination is elevated to DOJ leadership. And when there is "genuine uncertainty" on that question, the attorney general must make the call, a key political check.

Under the currently applicable DOJ Guidelines, even if you believed that a criminal case could have been made out against Mr. Burke for his lawful use of a publicly disclosed credential to log into a public website and obtain information that was publicly addressable, before resorting to applying for a search warrant, DOJ employees are required to go through the following analysis.

1. Are the records those of a member of the news media? In this case, the answer is an unqualified yes. Not only is Mr. Burke a journalist, but the records sought relate specifically to his collection and dissemination of newsworthy information. The records are also records of other journalists who work collaboratively with Mr. Burke. Mr. Burke, as an award winning member of the news media, is clearly within the scope of the policy. Moreover, the policy itself directs that if there is doubt on this question, the determination of such status must be approved by the assistant attorney general for the Criminal Division.

2. Is the member of the news media acting "within the scope of newsgathering"? The DOJ guidelines define newsgathering as the "process by which a member of the news media collects, pursues, or obtains information or records for purposes of producing content intended for public dissemination." Mr. Burke's overall activities, and the activities which led to the investigation involved the collection of information for the purposes of producing content which was then disseminated to the public. In short, this was within the scope of newsgathering, and the investigation was initiated as a leak investigation to determine the source of the information that was published. We note that 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," but as applied, this subsumes the definition of "newsgathering." Even if you believe that the manner in which Mr. Burke was collecting information was unlawful, he clearly was a journalist engaged in activities directed at gathering newsworthy information for dissemination to the public. Thus, if Mr. Burke actually engaged in criminal activity, then an argument could be made

---

https://www.npr.org/2021/10/14/1046124278/missouri-newspaper-security-flaws-hacking-investigation-gov-mike-parson Similarly, Wisconsin prosecutors threatened to prosecute NBC News reporter Mike Hixenbaugh for publishing lawfully acquired records related to child abuse. Molly Beck, Wisconsin Gov. Tony Evers' administration threatened to prosecute reporter over confidential child abuse records, Milwaukee Journal Sentinel October 14, 2020, https://www.jsonline.com/story/news/politics/2020/02/04/gov-tony-evers-administration-threatened-prosecution-journalist/2855362001/

that this was not "newsgathering." If he did not, then his activities were protected "newsgathering." While we fully contend that Mr. Burke did not engage in "unlawfully accessing a computer or computer system" -- especially as that term has been defined by the Supreme Court in *Van Buren,* even taken in a light most advantageous to the prosecution,this is a "close question" of whether Mr. Burke's actions in gathering information for publication from public sites is "newsgathering" under the regulation.

3. Does the "Criminal Activity" Exception Apply? The guidelines, as revised under Attorney General Garland, set up a new procedure to resolve this "close or novel" question to determine whether process is permitted. When there is a close or novel question regarding whether a journalist is acting "within the scope of newsgathering," it is elevated to the assistant attorney general for the Criminal Division, currently AAG Ken Polite. When the assistant attorney general finds there is "genuine uncertainty," the decision is elevated to Attorney General Garland. If the activity is within the scope of newsgathering, the process is barred completely (unless the narrow exceptions in § 50.10(c) apply). If the activity is not within the scope of newsgathering, and the journalist is the subject or target of an investigation, and suspected of committing an offense, the journalist is then subject to process under § 50.10(d)(1)(i) of the guidelines. Finally, under Section 50.10(d)(2)(ii), Attorney General approval is mandated as a prerequisite whenever anyone in the DOJ " seek[s] a search warrant for the premises of a news media entity…" In this case, Attorney General personal approval was a necessary prerequisite for the application for the warrant, and the affidavit in support of the warrant undoubtedly referenced whether or not such AG approval was sought and granted.

Thus, DAAG approval at a minimum would have been necessary for ANY compulsory process, and AG approval for the warrant to search and seize Mr. Burke's newsroom. In addition, DOJ suggests that the Criminal Division's CCIPS approve any searches for electronic records of journalists that implicate the Privacy Protection Act. [47]

E. The Affidavit May Not Have Complied With CCIPS Guidance

This same CCIPS manual also dictates that, drafting an affidavit in support of a warrant to conduct a search that implicates the Privacy Protection Act, agents and prosecutors should "explain both the search strategy and the practical considerations underlying the strategy in the affidavit." The manual notes that "[t]he affidavit should also explain what techniques the agents

[47] Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations, Computer Crime and Intellectual Property Section Criminal Division, page 101-109 (" Agents and prosecutors who have reason to believe that a computer search may implicate the [Privacy Protection Act] should contact the Computer Crime and Intellectual Property Section at (202) 514-1026 or the CHIP in their district (see Introduction, p. xix) for more specific guidance.") https://www.justice.gov/file/442111/download

expect to use to search the computer for the specific files that represent evidence of crime and may be intermingled with entirely innocuous documents. If the search strategy has been influenced by legal considerations such as potential PPA liability, the affidavit should explain how and why in the affidavit." [48] The CCIPS manual also notes:

> Agents contemplating a search that may result in the seizure of legally privileged computer files should devise a post-seizure strategy for screening out the privileged files and should describe that strategy in the affidavit. … the presiding judge may appoint a neutral third party known as a "special master" to the task of reviewing the files. Third, a team of prosecutors who are not working on the case may form a "taint team" or "privilege team" to help execute the search and review the files afterwards. The taint team sets up a so-called "Chinese Wall" between the evidence and the prosecution team, permitting only unprivileged files that are within the scope of the warrant to slip through the wall.

Since the government knew it was applying for a warrant to authorize the searching and seizing computers of a journalist related to the manner in which he collected information for publication, we expect that the affidavit in support of the warrant clearly advised the magistrate of this fact, and proposed (and the magistrate adopted and ordered) a procedure to minimize exposure by the prosecution team to this privileged information. Again, access to the affidavit in support of the warrant is necessary to determine whether this was done.

III. Summary and Conclusion

As we discussed, we reserve our rights to seek judicial review and remedy for what we firmly believe is a continuing infringement on Mr. Burke's First Amendment rights, right and ability to lawfully collect and disseminate newsworthy content, and prior restraint on speech. We are happy to work with you on the issues above to return as much content to Mr. Burke as possible, but we fundamentally disagree on the core issue -- whether Mr. Burke's activities were unlawful. To date, we have seen no indication whatsoever that they are on any reasonable interpretation of either the CFAA or the wiretap laws. It is our firm belief that all of the information about which Mr. Burke reported was obtained from sources that were either publicly accessible, or configured in a way as to be accessible to the public - irrespective of whether those who hosted or created this information knew that the data was so accessible. In that context, neither the CFAA nor the wiretap law precludes its access, "interception," or disclosure, and those actions are protected under the First Amendment.

---

[48] http://neiassociates.org/ccips/

Once again, declining to provide the otherwise public affidavit in support of the warrant forces us to make assumptions about what this case is actually about, and what theory of criminal liability was proposed to and tacitly accepted by the magistrate. Put simply, we are aware of no violation of law by Mr. Burke, based on the information and investigation we have conducted to date, and we firmly believe that the continued possession by the government of Mr. Burke's newsroom is an affront to the First Amendment. We want to resolve this quickly --not just procedurally, but substantially as well, and continue to offer to provide a lawyer's proffer if we can understand WHY you think Mr. Burke's journalism is criminal.

Yours truly,

Mark Rasch
Michael Maddux

Cc: Timothy Burke